Deutscher Bundestag
11. Wahlperiode

Drucksache 11/3730

13. 12. 88

Sachgebiet 204

Gesetzentwurf

der Abgeordneten Wartenberg (Berlin), Dr. Penner, Dr. Nöbel, Bernrath, Dr. Emmerlich, Graf, Hämmerle, Lambinus, Lutz, Paterna, Schröer (Mülheim), Dr. Sonntag-Wolgast, Tietjen, Peter (Kassel), Schütz, Dr. Skarpelis-Sperk, Vahlberg, Weiler, Wiefelspütz, Dr. Vogel und der Fraktion der SPD

Entwurf eines Gesetzes zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz — BISG)

A. Problem

Nach der grundlegenden Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 (BVerfGE 65,1) zum Volkszählungsgesetz wird der Schutz des einzelnen gegen unbegrenzte Verarbeitung und Nutzung seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Artikels 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG umfaßt. Dieses Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (Recht auf informationelle Selbstbestimmung). In der Zwischenzeit hat das Bundesverfassungsgericht in mehreren Entscheidungen diese Rechtsprechung bekräftigt. Das Gericht hat in seinem Beschluß vom 9. März 1988 (1 BvL 49/86) darüber hinaus klargestellt, daß das Recht auf informationelle Selbstbestimmung wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten schützt, unabhängig davon, ob die Daten in einer Datei verarbeitet werden.

Das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. Der einzelne muß vielmehr Einschränkungen dieses Rechts im überwiegenden Allgemeininteresse hinnehmen. Solche Beschränkungen bedürfen aber nach Artikel 2 Abs. 1 GG einer den Anforderungen der Normenklarheit entsprechenden gesetzlichen Grundlage und müssen dem Prinzip der Verhältnismäßigkeit genügen. Es verlangt, daß eine Grundrechtsbeschränkung von hinreichenden Gründen des Gemeinwohls gerechtfertigt wird, das gewählte Mittel zur Erreichung des Zwecks geeignet und

erforderlich ist und bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe, die Grenze des Zumutbaren noch gewahrt ist (vgl. BVerfGE 71, 183ff.). Daraus folgt, daß gesetzliche Regelungen erforderlich sind, die es dem einzelnen ermöglichen, das Selbstbestimmungsrecht über seine Daten wirksam auszuüben, und die die Voraussetzungen festlegen, unter denen er Einschränkungen dieses Rechts im überwiegenden Allgemeininteresse hinzunehmen hat.

Diesen verfassungsrechtlichen Anforderungen genügt das geltende Bundesdatenschutzgesetz erkennbar nicht.

B. Lösung

Das Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz — BDSG) vom 27. Januar 1977 (BGBl. I S. 201) wird grundlegend novelliert.

Der vorgelegte Entwurf eines Gesetzes zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz — BISG), das an die Stelle des geltenden Bundesdatenschutzgesetzes treten soll, hat das Ziel,

— das Bundesdatenschutzgesetz den vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Anforderungen an die Datenverarbeitung anzupassen,

— in der Praxis erkennbar gewordene Mängel des Gesetzes zu beseitigen und

— das Gesetz neuen technischen Entwicklungen anzupassen.

Insbesondere werden

— die Rechte der Betroffenen zum Beispiel durch die Einführung eines unentgeltlichen Auskunftsrechts sowie eines verschuldensunabhängigen Schadensersatzanspruchs maßgeblich verstärkt und erweitert,

— die Transparenz der Datenverarbeitung erhöht,

— die Rechtsstellung der Kontrollinstanzen verbessert und ihre Befugnisse erweitert,

— Sondervorschriften für die Verarbeitung von Arbeitnehmerdaten, die Datenverarbeitung für wissenschaftliche Zwecke, die Datenverarbeitung der Medien, über Datenschutzbeauftragte der Rundfunkanstalten des Bundesrechts, über Fernmessen und Fernwirken sowie über Video-Überwachung und -Aufzeichnung geschaffen.

Der Gesetzentwurf gibt dem einzelnen die Möglichkeit, über die Preisgabe und Verwendung seiner Daten zu bestimmen, indem er grundsätzlich die Erhebung beim Betroffenen vorschreibt und eine Verwendung verbietet, die nicht dem Erhebungszweck entspricht. Die im übrwiegenden Allgemeininteresse erforderlichen Ausnahmen von diesen Grundsätzen werden im Gesetzentwurf für jeden

erkennbar geregelt. Da der Betroffene seine Rechte nur wirksam ausüben kann, wenn er von der Verwendung seiner Daten Kenntnis hat, verstärkt der Entwurf die Aufklärungspflichten. Für Akten, Dateien und automatisierte Verfahren sind differenzierte und abgestufte Regelungen vorgesehen.

Parallel dazu sollen die Vorschriften des Verwaltungsverfahrensgesetzes, soweit diese für den Umgang mit personenbezogenen Daten von Bedeutung sind, geändert werden.

C. Alternativen

keine

D. Kosten

Der vorgesehene Ausbau der datenschutzrechtlichen Regelungen wird mittelbar zusätzliche Kosten mit sich bringen. Diese Mehrkosten sind zum gegenwärtigen Zeitpunkt nicht quantifizierbar, weil die Belastungen je nach den besonderen Verhältnissen ganz unterschiedlich ausfallen können; sie erreichen aber allenfalls eine finanziell begrenzte Größenordnung, da es sich nur um die Erweiterung einer bereits bestehenden Aufgabe handelt. Kosten entstehen vor allem durch die vorgesehene Höhergruppierung des Bundesbeauftragten für den Datenschutz von der Besoldungsgruppe B 9 in die Besoldungsgruppe B 10 (entsprechend der Besoldung des Wehrbeauftragten des Deutschen Bundestages) sowie durch die vorgesehene Ausweitung der Befugnisse der Aufgaben des Bundesbeauftragten für den Datenschutz.

Entwurf eines Gesetzes zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz — BISG)

Inhaltsübersicht

Seite

Artikel 1: Gesetz zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz — BISG)

Erster Abschnitt: Allgemeine Vorschriften

§ 1 Aufgabe und Regelungsbereich des Gesetzes 6
§ 2 Begriffsbestimmungen 6
§ 3 Zulässigkeit der Datenverarbeitung und Nutzung 7
§ 4 Automatisiertes Abrufverfahren und regelmäßige Datenübermittlungen 7
§ 5 Rechte der Betroffenen 7
§ 6 Schadensersatz 7
§ 7 Datengeheimnis 8
§ 8 Technische und organisatorische Maßnahmen 8
§ 9 Datenbeschreibung und Geräteverzeichnis 8

Zweiter Abschnitt: Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen

§ 10 Anwendungsbereich 9
§ 11 Verarbeitung personenbezogener Daten im Auftrag 9
§ 12 Datenerhebung 9
§ 13 Zweckbindung bei Verarbeitung, Veränderung und sonstiger Nutzung 10
§ 14 Datenübermittlung innerhalb des öffentlichen Bereichs 10
§ 15 Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften 11
§ 16 Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs . 11
§ 17 Datenübermittlung an öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes 11
§ 18 Auskunft an den Betroffenen, Benachrichtigung, Akteneinsicht ... 11
§ 19 Berichtigung, Sperrung und Löschung von Daten 12
§ 20 Durchführung des Schutzes personenbezogener Daten in der Bundesverwaltung 12
§ 21 Allgemeine Verwaltungsvorschriften 12
§ 22 Wahl des Bundesbeauftragten für den Datenschutz 12
§ 23 Rechtsstellung des Bundesbeauftragten für den Datenschutz 13
§ 24 Aufgaben des Bundesbeauftragten für den Datenschutz 13
§ 25 Verschwiegenheitspflicht 14
§ 26 Register für automatisiert geführte Dateien 14
§ 27 Beanstandungen durch den Bundesbeauftragten für den Datenschutz 14
§ 28 Anrufung des Bundesbeauftragten für den Datenschutz 14

Seite

Dritter Abschnitt: Datenverarbeitung nichtöffentlicher Stellen für eigene Zwecke

§ 29 Anwendungsbereich ... 15
§ 30 Datenerhebung, -speicherung und -nutzung ... 15
§ 31 Datenübermittlung ... 15
§ 32 Datenveränderung ... 15
§ 33 Datenverarbeitung im Rahmen des Arbeitsverhältnisses ... 16
§ 34 Benachrichtigung, Auskunft an den Betroffenen ... 16
§ 35 Berichtigung, Sperrung und Löschung von Daten ... 17
§ 36 Bestellung eines Beauftragten für den Datenschutz ... 17
§ 37 Aufgaben des Beauftragten für den Datenschutz ... 18
§ 38 Aufsichtsbehörde ... 18

Vierter Abschnitt: Geschäftsmäßige Datenverarbeitung nichtöffentlicher Stellen für fremde Zwecke

§ 39 Anwendungsbereich ... 19
§ 40 Datenerhebung, -speicherung, -übermittlung und -nutzung ... 19
§ 41 Datenveränderung ... 20
§ 42 Benachrichtigung, Auskunft an den Betroffenen, Einsicht ... 20
§ 43 Berichtigung, Sperrung und Löschung von Daten ... 20
§ 44 Datenerhebung und -speicherung zum Zweck der Direktwerbung . 20
§ 45 Datenübermittlung zum Zweck der Direktwerbung ... 21
§ 46 Rechte des Betroffenen bei der Direktwerbung ... 21
§ 47 Verarbeitung personenbezogener Daten zum Zweck der Übermittlung in anonymisierter Form ... 21
§ 48 Verarbeitung personenbezogener Daten im Auftrag ... 21
§ 49 Beauftragter für den Datenschutz ... 21
§ 50 Meldepflichten ... 21
§ 51 Aufsichtsbehörde ... 22

Fünfter Abschnitt: Besondere Vorschriften

§ 52 Datenverarbeitung für wissenschaftliche Zwecke ... 22
§ 53 Datenverarbeitung der Medien ... 22
§ 54 Datenschutzbeauftragter der Rundfunkanstalten des Bundesrechts . 23
§ 55 Fernmessen und Fernwirken ... 23
§ 56 Video-Überwachung und -Aufzeichnung ... 23

Sechster Abschnitt: Straf- und Bußgeldvorschriften

§ 57 Straftaten ... 23
§ 58 Ordnungswidrigkeiten ... 24

Artikel 2: Änderung des Verwaltungsverfahrensgesetzes

Artikel 3: Änderung des Gesetzes über das Bundesverfassungsgericht

Artikel 4: Berlin-Klausel

Artikel 5: Inkrafttreten

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

Artikel 1

Gesetz zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz — BISG)

ERSTER ABSCHNITT

Allgemeine Vorschriften

§ 1

Aufgabe und Regelungsbereich des Gesetzes

(1) Aufgabe dieses Gesetzes ist es, die Verarbeitung personenbezogener Daten zu regeln, um das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Informationen (Daten) zu bestimmen (informationelles Selbstbestimmungsrecht), soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind.

(2) Dieses Gesetz schützt personenbezogene Informationen (Daten), die

1. von Behörden oder sonstigen öffentlichen Stellen (§ 10),
2. von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts für eigene geschäftliche oder gewerbliche Zwecke (§ 29),
3. von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts geschäftsmäßig für fremde Zwecke (§ 39)

in Dateien oder Akten verarbeitet werden.

(3) Soweit besondere Rechtsvorschriften des Bundes auf die Verarbeitung oder sonstige Nutzung personenbezogener Informationen anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

§ 2

Begriffsbestimmungen

(1) Personenbezogene Daten im Sinne dieses Gesetzes sind Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Im Sinne dieses Gesetzes ist Datenverarbeitung das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten. Im einzelnen ist

1. Erheben (Erhebung) das Beschaffen von Daten beim Betroffenen oder bei anderen Personen oder Stellen,
2. Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung,
3. Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, daß Daten durch die speichernde Stelle an den Dritten weitergegeben werden oder daß der Dritte zum Abruf bereitgehaltene Daten abruft,
4. Sperren (Sperrung) das Verhindern weiterer Verarbeitung oder Nutzung gespeicherter Daten,
5. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten,
6. Nutzen (Nutzung) jede sonstige Verwendung personenbezogener Daten,
7. Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten,
8. Anonymisieren (Anonymisierung) das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,

ungeachtet der dabei angewendeten Verfahren.

(3) Im Sinne dieses Gesetzes ist

1. datenverarbeitende Stelle jede der in § 1 Abs. 2 genannten Personen oder Stellen, die Daten ausschließlich oder auch für sich selbst speichert oder durch andere speichern läßt,
2. Dritter jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die in den Fällen der Nummer 1 im Geltungsbereich dieses Gesetzes im Auftrag tätig werden,
3. eine Datei
   a) eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei) oder
   b) eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren,
4. eine Akte jede amtlichen oder geschäftlichen Zwecken dienende Unterlage. Dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

§ 3

Zulässigkeit der Datenverarbeitung und Nutzung

(1) Die Verarbeitung und sonstige Nutzung personenbezogener Daten ist nur zulässig, wenn

1. dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
2. der Betroffene eingewilligt hat.

(2) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist der Betroffene auf die Einwilligungserklärung schriftlich besonders hinzuweisen.

(3) Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung auch über die Empfänger der Daten aufzuklären; er ist unter Hinweis auf die Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern kann.

(4) Die Einwilligung ist unwirksam, wenn sie durch unangemessene Androhung von Nachteilen, durch fehlende Aufklärung oder in sonstiger, gegen die Gebote von Treu und Glauben verstoßender Weise bewirkt wurde. Wird die Einwilligung im Rahmen von allgemeinen Geschäftsbedingungen erklärt, ist sie nur insoweit wirksam, als die Datenverarbeitung, in die eingewilligt wurde, im Hinblick auf den Vertragszweck angemessen ist.

§ 4

Automatisiertes Abrufverfahren und regelmäßige Datenübermittlungen

(1) Personenbezogene Daten dürfen zum Abruf in automatisierten Verfahren nur bereitgehalten werden, wenn verbindlich festgelegt ist, wer welche Daten für welchen Zweck abrufen darf, und wenn angemessene Maßnahmen zur Sicherung und Kontrolle auch beim Empfänger getroffen sind. Insbesondere muß gewährleistet sein, daß die Daten nur für den zugelassenen Zweck abgerufen und daß die Erforderlichkeit des Abrufs kontrolliert werden kann.

(2) Im Bereich der öffentlichen Stellen des Bundes im Sinne des § 10 Abs. 1 Satz 1 darf ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte nur eingerichtet werden, wenn eine Rechtsvorschrift dies zuläßt. Die Bundesminister werden ermächtigt, nach Maßgabe des Absatzes 1 automatisierte Abrufverfahren für ihren Geschäftsbereich durch Rechtsverordnung einzuführen, wenn das Bereithalten der Daten zum sofortigen Abruf durch den Empfänger unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgabe der beteiligten Stellen angemessen ist.

(3) Personenbezogene Daten dürfen von öffentlichen Stellen zum Abruf in automatisierten Verfahren für Personen oder Stellen außerhalb des öffentlichen Bereichs nicht bereitgehalten werden.

(4) Die Absätze 1 bis 3 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung zur Abfrage offenstehen oder deren Veröffentlichung zulässig wäre.

(5) Die Absätze 1 und 2 sind auf die Zulassung regelmäßiger Datenübermittlungen entsprechend anzuwenden.

§ 5

Rechte des Betroffenen

(1) Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. kostenlose Auskunft über die zu seiner Person gespeicherten Daten,
2. Berichtigung, Löschung oder Sperrung der zu seiner Person gespeicherten Daten,
3. Schadensersatz,
4. Einsicht in die beim Bundesbeauftragten für den Datenschutz und bei den Aufsichtsbehörden geführten Register,
5. Anrufung des Bundesbeauftragten für den Datenschutz bzw. der zuständigen Aufsichtsbehörde.

(2) Die in Absatz 1 genannten Rechte des Betroffenen können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

§ 6

Schadensersatz

(1) Wird der Betroffene durch eine unzulässige oder unrichtige automatisierte Verarbeitung personenbezogener Daten in seinen schutzwürdigen Belangen beeinträchtigt, so hat ihm der Träger der datenverarbeitenden Stelle unabhängig von einem Verschulden den Schaden zu ersetzen. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Der Ersatzpflichtige haftet jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von 500 000 Deutsche Mark.

(2) Sind bei einer Datei mehrere Stellen verarbeitungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(3) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(4) Auf das Mitverschulden des Verletzten und die Verjährung des Entschädigungsanspruchs sind die §§ 254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(5) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang als nach dieser Vorschrift oder nach

denen ein anderer für den Schaden verantwortlich ist, bleiben unberührt.

(6) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

§ 7

Datengeheimnis

(1) Den im Rahmen des § 1 Abs. 2 oder im Auftrag dort genannter Personen oder Stellen bei der Datenverarbeitung beschäftigten Personen ist untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen. Diese Pflichten bestehen auch nach Beendigung der Tätigkeit fort.

(2) Die Personen, die bei datenverarbeitenden Stellen nach § 1 Abs. 2 Nr. 2 und 3 beschäftigt sind, sind bei Aufnahme ihrer Tätigkeit nach Maßgabe von Absatz 1 zu verpflichten.

§ 8

Technische und organisatorische Maßnahmen

(1) Wer im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Stellen personenbezogene Daten verarbeitet, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. Die Art und Weise der Maßnahmen richtet sich nach dem jeweiligen Stand der Technik. Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(2) Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungssystemen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4. die Benutzung von Datenverarbeitungssystemen mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte zu verhindern (Benutzerkontrolle),
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, daß überprüft und festgestellt werden kann, an wen wann welche personenbezogenen Daten durch Einrichtungen zur Datenübertragung übermittelt worden sind (Übermittlungskontrolle),
7. zu gewährleisten, daß überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu gewährleisten, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert, gelöscht oder entfernt werden können (Transportkontrolle).

(3) Werden personenbezogene Daten in nicht automatisierten Dateien oder in Akten verarbeitet, sind die nach Absatz 1 erforderlichen Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

§ 9

Dateibeschreibung und Geräteverzeichnis

(1) Die datenverarbeitende Stelle ist verpflichtet, in einer Beschreibung jeder Datei festzulegen:

1. die Zweckbestimmung der Datei,
2. die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,
3. den Kreis der Betroffenen,
4. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Art und die Herkunft regelmäßig empfangener Daten,
5. Fristen für die Sperrung und Löschung der Daten,
6. die technischen und organisatorischen Maßnahmen nach § 8,
7. bei automatisierten Verfahren die Betriebsart des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.

(2) Absatz 1 findet keine Anwendung auf nicht automatisierte Dateien, deren Daten nicht zur Übermittlung bestimmt sind.

(3) Die datenverarbeitende Stelle oder die in ihrem Auftrag tätige Stelle ist verpflichtet, in einem Verzeichnis der Geräte, mit denen personenbezogene Daten automatisiert verarbeitet werden, festzulegen:

1. den Typ und die Art der Geräte,
2. den Hersteller,
3. die Anzahl und den Standort der Geräte,
4. das verwendete Betriebssystem,
5. die Möglichkeiten zur Datenfernverarbeitung und Datenübertragung,
6. verwendete Standard- und Anwenderprogramme.

Das Verzeichnis ist laufend auf dem neuesten Stand zu halten. Weitere in das Verzeichnis aufzunehmende Angaben über die Ausstattung der Geräte und deren Verwendung bestimmt die Bundesregierung durch Rechtsverordnung mit Zustimmung des Bundesrates.

ZWEITER ABSCHNITT

Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen

§ 10

Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für Behörden und sonstige öffentliche Stellen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie für Vereinigungen solcher Körperschaften, Anstalten und Stiftungen. Für öffentlich-rechtliche Unternehmen, soweit sie am Wettbewerb teilnehmen, gelten von den Vorschriften dieses Abschnittes jedoch nur die §§ 20 bis 28.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die Vorschriften dieses Abschnittes mit Ausnahme der §§ 20 bis 28 auch für

1. Behörden und sonstige öffentliche Stellen der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen, soweit sie Bundesrecht ausführen,
2. Behörden und sonstige öffentliche Stellen der Länder, soweit sie als Organe der Rechtspflege tätig werden, ausgenommen in Verwaltungsangelegenheiten.

Für öffentlich-rechtliche Unternehmen, soweit sie am Wettbewerb teilnehmen und soweit sie die Voraussetzungen von Satz 1 Nr. 1 erfüllen, gelten die Vorschriften dieses Abschnittes nicht.

(3) Abweichend von den Absätzen 1 und 2 gelten anstelle der §§ 12 bis 19 die §§ 30 bis 35 entsprechend, soweit die Datenverarbeitung frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse betrifft.

§ 11

Verarbeitung personenbezogener Daten im Auftrag

(1) Die Vorschriften dieses Abschnittes gelten für die in § 10 Abs. 1 und 2 genannten Stellen auch insoweit, als personenbezogene Daten in deren Auftrag durch andere Personen oder Stellen verarbeitet werden. In diesen Fällen ist der Auftraggeber unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 8 Abs. 1) sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Art der Datenverarbeitung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse konkret zu beschreiben sind.

(2) Die Vorschriften dieses Abschnittes gelten mit Ausnahme der §§ 20 bis 28 nicht für die in § 10 Abs. 1 und 2 genannten Stellen, soweit sie personenbezogene Daten im Auftrag verarbeiten. In diesen Fällen ist die Verarbeitung personenbezogener Daten nur im Rahmen der Weisungen des Auftraggebers zulässig.

(3) Für juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen dem Bund oder einer bundesunmittelbaren Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, gelten die §§ 20 bis 28 entsprechend, soweit diese Personen oder Personenvereinigungen in den Fällen des Absatzes 1 Satz 1 im Auftrag tätig werden.

§ 12

Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn diese Daten zur rechtmäßigen Erfüllung der Aufgaben der erhebenden Stelle oder der Stelle, für die die Daten beschafft werden, erforderlich sind.

(2) Personenbezogene Daten dürfen grundsätzlich nur beim Betroffenen mit seiner Kenntnis erhoben werden. Durch die Art und Weise der Erhebung dürfen schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

(3) Werden Daten beim Betroffenen erhoben, so ist er über den Verwendungszweck aufzuklären. Bei beabsichtigten Übermittlungen umfaßt die Aufklärungspflicht auch die Angabe des Empfängers der Daten. Werden Daten beim Betroffenen aufgrund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, so ist er in verständlicher Form auf sie, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Werden vom Betroffenen freiwillige Angaben erbeten, so ist er über mögliche Folgen einer Nichtbeantwortung aufzuklären.

(4) Das Erheben personenbezogener Daten bei einer anderen öffentlichen Stelle ist nur unter den Voraussetzungen des § 13 Abs. 2 zulässig.

(5) Bei Dritten außerhalb des öffentlichen Bereichs dürfen personenbezogene Daten im Einzelfall ohne

Kenntnis des Betroffenen nur erhoben werden, wenn eine Rechtsvorschrift dies erlaubt oder zwingend voraussetzt oder wenn der Schutz von Leben oder Gesundheit dies gebietet.

(6) Werden personenbezogene Daten beim Betroffenen ohne seine Kenntnis erhoben, so ist er davon zu benachrichtigen, sobald die rechtmäßige Erfüllung der Aufgaben dadurch nicht mehr gefährdet wird. Die Benachrichtigung umfaßt die Angabe der Rechtsgrundlage, die Aufklärung über den Zweck der Datenerhebung und bei Übermittlungen auch den Empfänger der Daten.

§ 13

Zweckbindung bei Verarbeitung, Veränderung und sonstiger Nutzung

(1) Das Speichern, Verändern und Nutzen personenbezogener Daten ist zulässig, wenn es zur rechtmäßigen Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist. Personenbezogene Daten dürfen grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind.

(2) Die Verwendung für andere Zwecke ist nur zulässig, wenn

1. der Betroffene eingewilligt hat,
2. eine Rechtsvorschrift dies erlaubt,
3. hierdurch erhebliche Nachteile für das Gemeinwohl oder eine schwerwiegende Beeinträchtigung der Rechte einzelner verhindert oder beseitigt werden sollen,
4. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben,
5. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, die Verarbeitung im Interesse des Betroffenen liegt und davon ausgegangen werden kann, daß dieser in Kenntnis des Verwendungszwecks seine Einwilligung hierzu erteilt hätte, oder
6. die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen sind, es sei denn, daß schutzwürdige Belange des Betroffenen offensichtlich entgegenstehen.

Besondere Amts- und Berufsgeheimnisse bleiben unberührt.

(3) Die Wahrnehmung von Aufsichts- und Kontrollbefugnissen, die Rechnungsprüfung und die Verarbeitung zu Ausbildungs- und Prüfungszwecken gelten nicht als Verarbeitung für andere Zwecke.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

§ 14

Datenübermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten durch eine öffentliche Stelle an eine andere öffentliche Stelle im Geltungsbereich des Grundgesetzes ist zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und die Voraussetzungen des § 13 Abs. 1 oder des § 13 Abs. 2 vorliegen. Die Übermittlung ist ferner zulässig, soweit es zur Entscheidung in einem Verwaltungsverfahren der Beteiligung mehrerer öffentlicher Stellen bedarf.

(2) Unterliegen die personenbezogenen Daten einem Berufs- oder einem besonderen Amtsgeheimnis und sind sie der öffentlichen Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der weiteren Übermittlung stets erforderlich, daß der Empfänger die Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die übermittelnde Stelle erhalten hat.

(3) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(4) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung zur Erfüllung von Aufgaben des Empfängers, so trägt auch dieser hierfür die Verantwortung und hat sicherzustellen, daß die Erforderlichkeit nachträglich überprüft werden kann. Die übermittelnde Stelle hat in diesem Fall die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen. Bestehen im Einzelfall Zweifel an der Schlüssigkeit, so hat sie darüber hinaus die Erforderlichkeit zu überprüfen. Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen. Erfolgt die Übermittlung durch automatisierten Abruf (§ 4), so trägt die Verantwortung für die Rechtmäßigkeit des Abrufs allein der Empfänger.

(5) Der Empfänger darf die übermittelten Daten nur für den Zweck verwenden, zu dem sie ihm übermittelt worden sind; § 13 Abs. 2 findet entsprechende Anwendung.

(6) Die Absätze 1 bis 5 gelten entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 15

Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgemeinschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an öffentliche Stellen zulässig, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Maßnahmen zum Schutz personenbezogener Daten getroffen werden.

§ 16

Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Personen und an andere als die in § 14 genannten Stellen ist zulässig, wenn

1. sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen von § 13 Abs. 1 vorliegen,
2. sie unter den Voraussetzungen des § 13 Abs. 2 Nr. 1, 4 oder 6 für andere Zwecke verwendet werden dürfen oder
3. der Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(2) Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der öffentlichen Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der Übermittlung ferner erforderlich, daß die gleichen Voraussetzungen gegeben sind, unter denen sie die zur Verschwiegenheit verpflichtete Person übermitteln durfte.

(3) Der Empfänger darf die übermittelten Daten nur für den Zweck verwenden, zu dem sie ihm übermittelt worden sind.

§ 17

Datenübermittlung an öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes

Auf die Übermittlung an öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen ist § 16 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen entsprechend anzuwenden. Der Empfänger ist zu verpflichten, die übermittelten Daten nur zu dem Zweck zu verwenden, zu dem sie ihm übermittelt worden sind. Die Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines deutschen Gesetzes verstoßen würde oder schutzwürdige Belange des Betroffenen verletzt würden.

§ 18

Auskunft an den Betroffenen, Benachrichtigung, Akteneinsicht

(1) Dem Betroffenen ist von der datenverarbeitenden Stelle auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Speicherung sowie
3. die Herkunft der Daten und die Empfänger von Übermittlungen,

auch soweit diese Angaben nicht zu seiner Person gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können. Der Betroffene soll die Art der personenbezogenen Daten, über die er Auskunft verlangt, näher bezeichnen.

(2) Werden personenbezogene Daten in einer automatisierten Datei gespeichert, so ist der Betroffene von dieser Tatsache schriftlich zu benachrichtigen. Die Benachrichtigung umfaßt die nach § 9 Abs. 1 Nr. 1 bis 5 festzulegenden Angaben; sie kann zusammen mit der Erhebung erfolgen. Spätere Änderungen dieser Angaben sind ihm ebenfalls mitzuteilen.

(3) Die Verpflichtung zur Auskunftserteilung gilt nicht für die personenbezogenen Daten, die nur deshalb als gesperrte Daten gespeichert sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, sowie für solche Daten, die ausschließlich zum Zwecke der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(4) Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, kann er bei der datenverarbeitenden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die personenbezogenen Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall kann ihm statt Einsicht Auskunft gewährt werden.

(5) Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Akteneinsicht entfällt, soweit

1. dies die ordnungsgemäße Erfüllung der Aufgaben der datenverarbeitenden Stelle gefährden würde,
2. dies die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der berech-

tigten Interessen einer dritten Person, geheimgehalten werden müssen.

(6) Die Verweigerung der Auskunft oder der Akteneinsicht ist zu begründen. Dies gilt nicht, wenn durch die Mitteilung der Gründe der mit der Verweigerung verfolgte Zweck gefährdet würde; die wesentlichen Gründe für die Entscheidung sind aufzuzeichnen.

(7) Unterbleibt die Auskunft gegenüber dem Betroffenen, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen. Die Mitteilung des Bundesbeauftragten für den Datenschutz an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

§ 19

Berichtigung, Sperrung und Löschung von Daten

(1) Personenbezogene Daten sind unverzüglich zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt,
2. in den Fällen des Absatzes 3 Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt würden oder der Betroffene an Stelle der Löschung die Sperrung verlangt,
3. sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene in die Nutzung eingewilligt hat.

(3) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung ihrer Aufgaben nicht mehr erforderlich ist.

(4) Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Absatz 3 Nr. 2 nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist, es sei denn, daß der Betroffene die Löschung verlangt und die weitere Speicherung ihn in unangemessener Weise beeinträchtigen würde. Soweit hiernach eine Löschung nicht in Betracht kommt, sind die personenbezogenen Daten auf Antrag des Betroffenen zu sperren.

(5) Abgesehen von den Fällen des Absatzes 3 Nr. 1 besteht eine Verpflichtung zur Löschung nicht, soweit Rechtsvorschriften die Übergabe personenbezogener Daten an staatliche oder kommunale Archive anordnen.

(6) Über die Berichtigung unrichtiger Daten, die Sperrung bestrittener Daten und die Löschung oder Sperrung unzulässig gespeicherter Daten sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt worden sind. Die Unterrichtung kann unterbleiben, wenn sie einen erheblichen Aufwand erfordern würde und nachteilige Folgen für den Betroffenen nicht zu befürchten sind.

§ 20

Durchführung des Schutzes personenbezogener Daten in der Bundesverwaltung

Die obersten Bundesbehörden, der Vorstand der Deutschen Bundesbahn sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von einer obersten Bundesbehörde lediglich Rechtsaufsicht ausgeübt wird, haben jeweils für ihren Geschäftsbereich die Ausführung des Gesetzes sowie anderer Rechtsvorschriften über den Schutz personenbezogener Daten sicherzustellen.

§ 21

Allgemeine Verwaltungsvorschriften

Die obersten Bundesbehörden und der Vorstand der Deutschen Bundesbahn erlassen jeweils für ihren Geschäftsbereich allgemeine Verwaltungsvorschriften, die die Ausführung dieses Gesetzes, bezogen auf die besonderen Verhältnisse in dem jeweiligen Geschäftsbereich, und die sich daraus ergebenden besonderen Erfordernisse für den Schutz personenbezogener Daten regeln.

§ 22

Wahl des Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz wird auf 6 Jahre gewählt. Einmalige Wiederwahl ist zulässig.

(2) Die Bundesregierung schlägt dem Deutschen Bundestag spätestens 3 Monate vor Ablauf der Amtszeit des Bundesbeauftragten einen Bewerber für die nächste Amtszeit vor. Gewählt ist, wer die Stimmen von zwei Dritteln der Mitglieder des Bundestages erhält. Der Gewählte ist vom Bundespräsidenten zu ernennen.

(3) Der Präsident des Deutschen Bundestages verpflichtet den Bundesbeauftragten vor dem Deutschen Bundestag, sein Amt gerecht zu führen und das Grundgesetz und die Gesetze des Bundes zu wahren und zu verteidigen.

(4) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkunde. Der Bundesbeauftragte kann jederzeit von seinem Amt zurücktreten. Nach dem Ende seiner Amtszeit bleibt er bis zur Neuwahl im Amt.

(5) Der Deutsche Bundestag kann mit der Mehrheit seiner Mitglieder beim Bundesverfassungsgericht die Abberufung des Bundesbeauftragten für den Datenschutz aus den Gründen beantragen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Amt rechtfertigen. Für das Verfahren gelten Artikel 98 Abs. 2 des Grundgesetzes und § 58 Abs. 1 und 3, §§ 59 und 61 des Gesetzes über das Bundesverfassungsgericht entsprechend.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, so kann der Präsident des Deutschen Bundestages einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte ist dazu zu hören.

§ 23

Rechtsstellung des Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis. Er ist in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Dienstaufsicht des Präsidenten des Deutschen Bundestages.

(2) Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Deutschen Bundestages mit einem eigenen Kapitel auszuweisen.

(3) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(4) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluß des Kalendermonats , in dem das Amtsverhältnis endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 10 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im übrigen sind die §§ 13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kürzung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, daß an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von sechs Jahren tritt.

(5) Die Bediensteten werden auf Vorschlag des Bundesbeauftragten ernannt. Sie sind ausschließlich an seine dienstlichen Weisungen gebunden und können nur im Einvernehmen mit ihm versetzt oder abgeordnet werden.

§ 24

Aufgaben des Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz kontrolliert die Beachtung des Rechts auf informationelle Selbstbestimmung durch die öffentlichen Stellen des Bundes, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden und unterstützt den Deutschen Bundestag bei der Ausübung der parlamentarischen Kontrolle. Er berät die öffentlichen Stellen des Bundes bei der Verwirklichung der Rechtsvorschriften über den Schutz personenbezogener Daten.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung erstellt der Bundesbeauftragte für den Datenschutz Gutachten und erstattet Berichte zu Fragen des Datenschutzes und des freien Zugangs zu Informationen. Außerdem erstattet er dem Deutschen Bundestag regelmäßig im Januar eines jeden Jahres einen Tätigkeitsbericht. Er kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte beobachtet die Auswirkungen der neuen Informationstechniken auf die Arbeitsweise der öffentlichen Stellen des Bundes. Er ist über Planungen zum Aufbau neuer Informationssysteme rechtzeitig zu unterrichten.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu seinen Fragen sowie die Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, sowie
2. jederzeit Zutritt in alle Diensträume zu gewähren.

(5) Absatz 4 gilt auch hinsichtlich personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Das Post- und Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird eingeschränkt, soweit dies zur Ausübung der Kontrolle bei der Deutschen Bundespost erforderlich ist.

(6) Absatz 4 Sätze 1 und 2 gelten für die Behörden für Verfassungsschutz, den Bundesnachrichtendienst, den militärischen Abschirmdienst sowie andere Behörden des Bundesministers der Verteidigung, soweit die Sicherheit des Bundes berührt wird, das Bundeskriminalamt, die Behörden der Staatsanwaltschaft und der Polizei sowie die für Steuerfahndung zuständigen Behörden des Bundes und der Länder mit der Maßgabe, daß die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders damit Beauftragten zu gewähren ist. Personenbe-

zogene Daten eines Betroffenen, dem eine der in Satz 1 genannten Stellen Vertraulichkeit besonders zugesichert hat, müssen nicht offenbart werden.

(7) Der Bundesbeauftragte arbeitet mit den öffentlichen Stellen zusammen, die für die Kontrolle der Beachtung des Rechts auf informationelle Selbstbestimmung in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach §§ 38 und 51 dieses Gesetzes.

(8) Absatz 5 gilt entsprechend für die öffentlichen Stellen, die die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern durchführen.

§ 25

Verschwiegenheitspflicht

Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte ist oberste Dienstbehörde im Sinne des § 96 der Strafprozeßordnung und entscheidet nach §§ 61 und 62 BBG für sich und seine Beschäftigten in eigener Verantwortung.

§ 26

Register für automatisiert geführte Dateien

(1) Der Bundesbeauftragte führt ein Register aller automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert werden. Die öffentlichen Stellen des Bundes sind verpflichtet, die von ihnen geführten Dateien beim Bundesbeauftragten anzumelden. Das Register kann von jedermann eingesehen werden. Der Bundesbeauftragte erteilt auf Antrag schriftliche Auskunft aus dem Register für diejenigen Dateien, an deren Kenntnis der Antragsteller ein berechtigtes Interesse darlegt. Die Auskunft ist kostenfrei. Der Bundesbeauftragte veröffentlicht mindestens einmal im Jahr in geeigneter Form eine Übersicht über den Inhalt des Registers. Auf die Veröffentlichung der Übersicht ist im Bundesanzeiger hinzuweisen.

(2) Für die in § 24 Abs. 6 genannten Behörden gilt nur Absatz 1 Sätze 1 und 2; der Bundesbeauftragte führt für die Dateien dieser Behörden ein besonderes Register, das sich auf eine Übersicht über Art und Verwendungszweck beschränkt.

§ 27

Beanstandungen durch den Bundesbeauftragten für den Datenschutz

(1) Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Bestimmungen über den Schutz personenbezogener Daten oder sonstige Mängel fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber dem zuständigen Bundesminister,
2. bei der Deutschen Bundesbahn gegenüber dem Vorstand,
3. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 3 unterrichtet der Bundesbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt oder wenn ihre Behebung sichergestellt ist.

(3) Mit der Beanstandung kann der Bundesbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Absatz 1 Satz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 3 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

(5) Lehnt die nach Absatz 1 verantwortliche Stelle es ab, die vom Bundesbeauftragten festgestellten Verstöße zu beseitigen, so kann der Bundesbeauftragte verlangen, daß die Bundesregierung sich mit der Angelegenheit befaßt. Vor der Entscheidung der Bundesregierung dürfen personenbezogene Daten, deren Verarbeitung der Bundesbeauftragte beanstandet hat, nicht weiter verarbeitet werden.

§ 28

Anrufung des Bundesbeauftragten für den Datenschutz

(1) Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, durch die Verarbeitung oder Nutzung seiner personenbezogenen Daten durch die in § 10 Abs. 1 genannten öffentlichen Stellen des Bundes, ausgenommen der Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden, in seinen Rechten verletzt worden zu sein.

(2) Niemand darf wegen der Mitteilung von Tatsachen, die geeignet sind, den Verdacht aufkommen zu lassen, dieses Gesetz oder eine andere Rechtsvorschrift über den Schutz personenbezogener Daten sei verletzt worden, gemaßregelt oder benachteiligt werden. Beschäftigte des Bundes sind nicht verpflichtet, dem Bundesbeauftragten gegenüber den Dienstweg einzuhalten.

DRITTER ABSCHNITT

Datenverarbeitung nichtöffentlicher Stellen für eigene Zwecke

§ 29
Anwendungsbereich

(1) Die Vorschriften dieses Abschnitts gelten für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie geschützte personenbezogene Daten als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder Ziele verarbeiten oder nutzen. Sie gelten mit Ausnahme der §§ 36 bis 38 nach Maßgabe von Satz 1 auch für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, soweit sie die Voraussetzungen von § 10 Abs. 1 Satz 1 oder § 10 Abs. 2 Satz 1 Nr. 1 erfüllen.

(2) Die Vorschriften dieses Abschnitts gelten für die in Absatz 1 genannten Personen, Gesellschaften und anderen Personenvereinigungen auch insoweit, als personenbezogene Daten in deren Auftrag durch andere Personen oder Stellen verarbeitet werden. In diesen Fällen ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 8 Abs. 1) sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Art der Datenverarbeitung, die technisch organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse konkret zu beschreiben sind.

(3) Die Vorschriften dieses Abschnitts gelten nicht für die in Absatz 1 genannten Personen, Gesellschaften und anderen Personenvereinigungen, die Aufgaben der öffentlichen Verwaltung wahrnehmen.

§ 30
Datenerhebung, -speicherung und -nutzung

(1) Das Erheben, das Speichern und die sonstige Nutzung personenbezogener Daten ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Abweichend von Satz 1 ist das Speichern in nichtautomatisierten Verfahren zulässig, soweit die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen werden.

(2) Personenbezogene Daten sollen beim Betroffenen erhoben werden. Durch die Art und Weise der Erhebung dürfen schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

(3) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, dürfen nur für die Zwecke verwendet werden, zu denen sie gespeichert worden sind.

§ 31
Datenübermittlung

(1) Die Übermittlung personenbezogener Daten ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen. Wenn schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden, ist die Übermittlung auch zulässig, soweit es zur Wahrung berechtigter Interessen der übermittelnden Stelle, der Allgemeinheit oder eines Dritten erforderlich ist. Der Empfänger darf die übermittelten Daten nur für den Zweck verwenden, zu dem sie ihm übermittelt worden sind.

(2) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, dürfen vom Empfänger nicht weiter übermittelt werden.

(3) Abweichend von Absatz 1 dürfen Name, Titel, akademische Grade, Berufs- und Amtsbezeichnung, Anschrift und Rufnummer übermittelt werden

1. zur Herstellung von Verzeichnissen über Personen, die einem Verein oder einer Gesellschaft angehören, wenn die Satzung dies zuläßt,
2. zur Herstellung von Verzeichnissen über Angehörige bestimmter Berufsgruppen und zu ähnlichen Zwecken, wenn unter Berücksichtigung des Verwendungszusammenhangs und der Art der Daten kein Grund zu der Annahme besteht, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden,
3. zum Zweck der Markt- und Meinungsforschung, wenn die Angaben sich auf Personen beziehen, die in vertraglichen Beziehungen zu der speichernden Stelle stehen und die Übermittlung nicht nach dem Inhalt des Vertrages ausgeschlossen ist.

(4) In den Fällen des Absatzes 3 muß die Absicht der Übermittlung so bekanntgemacht werden, daß die Betroffenen Gelegenheit zum Widerspruch haben. Widerspricht der Betroffene der Übermittlung, so sind die ihn betreffenden Daten von der Übermittlung auszunehmen; sind sie bereits übermittelt, so hat der Empfänger sie unverzüglich zu löschen. Der Empfänger darf die Daten nur zu dem Zweck verwenden, zu dem sie ihm übermittelt worden sind.

§ 32
Datenveränderung

Das Verändern personenbezogener Daten ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

§ 33

Datenverarbeitung im Rahmen des Arbeitsverhältnisses

(1) Der Arbeitgeber darf personenbezogene Daten des Arbeitnehmers vor Abschluß des Arbeitsvertrages oder im Rahmen eines bestehenden Arbeitsvertrages abweichend von §§ 30 und 31 nur erheben, verarbeiten oder sonst nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich ist oder eine andere Rechtsvorschrift dies vorschreibt. Der Arbeitgeber darf vom Arbeitnehmer die Einwilligung für eine darüber hinausgehende Datenverarbeitung nicht verlangen. Besteht ein Personalfragebogen (§ 94 Abs. 1 Betriebsverfassungsgesetz), so beschränkt sich die Datenerhebung auf die darin enthaltenen Fragen; Gleiches gilt für persönliche Angaben in schriftlichen Arbeitsverträgen, die allgemein für den Betrieb verwendet werden (§ 94 Abs. 2 Betriebsverfassungsgesetz). Die Datenübermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

(2) Der Arbeitgeber darf beim Arbeitnehmer vor Abschluß des Arbeitsvertrages Daten über berufliche und fachliche Kenntnisse, Erfahrungen und Fähigkeiten erheben. Sonstige Daten, insbesondere hinsichtlich persönlicher und wirtschaftlicher Verhältnisse, darf der Arbeitgeber nur erheben, soweit die zu besetzende Arbeitsstelle oder die zu leistende Arbeit dies erfordert.

(3) Die Erhebung medizinischer Daten bei ärztlichen Untersuchungen des Arbeitnehmers vor Abschluß des Arbeitsvertrages ist nur zulässig, soweit dadurch seine Eignung für die von ihm zu leistende Arbeit festgestellt wird und er vorher sein Einverständnis zu Art und Umfang der Datenerhebung erteilt hat. Der untersuchende Arzt darf dem Arbeitgeber in der Regel nur das Ergebnis der Eignungsuntersuchung mitteilen.

(4) Die Erhebung psychologischer Daten in Zusammenhang mit der Eingehung eines Arbeitsverhältnisses ist nur zulässig, soweit sie wegen besonderer Anforderungen an den Arbeitnehmer im Hinblick auf die von ihm zu leistende Arbeit erforderlich ist, vorhandene Bewerbungsunterlagen zur Beurteilung nicht bereits ausreichen, der Arbeitnehmer zuvor über Art und Umfang der Datenerhebung informiert wurde und sein Einverständnis hierzu erklärt hat. Allgemeine Persönlichkeitstests sind nicht zulässig. Daten im Zusammenhang mit psychologischen Tests dürfen nur von Psychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung erhoben werden; sie sind nach Feststellung des Ergebnisses unverzüglich zu sperren. Dem Arbeitgeber darf nur das Ergebnis der psychologischen Untersuchung mitgeteilt werden.

(5) Die Ergebnisse medizinischer und psychologischer Untersuchungen des Arbeitnehmers dürfen automatisiert nur bearbeitet werden, wenn dies dem Schutz des Arbeitnehmers dient. Arbeitsrechtliche Beurteilungen dürfen nicht allein auf Daten gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

(6) Personenbezogene Daten, die vor der Eingehung eines Arbeitsverhältnisses erhoben wurden, sind, soweit sie nicht mit dem Datenträger an den Betroffenen zurückgegeben werden, unverzüglich zu löschen, sobald feststeht, daß ein Arbeitsverhältnis nicht zustande kommt, es sei denn, daß der Betroffene zur Aufrechterhaltung seiner Bewerbung in die weitere Speicherung eingewilligt hat. Nach Beendigung eines Arbeitsverhältnisses sind pesonenbezogene Daten des Beschäftigten auf seinen Antrag zu löschen, sobald feststeht, daß sie für die Abwicklung des Arbeitsverhältnisses nicht mehr benötigt werden und Rechtsvorschriften nicht entgegenstehen.

(7) Personenbezogene Daten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen gemäß § 8 gespeichert werden, dürfen nicht zu anderen Zwecken, insbesondere nicht zur individuellen Verhaltens- oder Leistungskontrolle verarbeitet oder sonst genutzt werden; auf Verlangen ist dem Beschäftigten Auskunft über die Art dieser Daten zu erteilen.

§ 34

Benachrichtigung, Auskunft an den Betroffenen

(1) Werden erstmals zur Person des Betroffenen Daten in Dateien gespeichert, ist er darüber zu benachrichtigen, wenn nicht auf andere Weise sichergestellt worden ist, daß er von der Speicherung eindeutig Kenntnis erlangen konnte. Dabei sind die Art der gespeicherten Daten und die Empfänger regelmäßiger Übermittlungen mitzuteilen. Werden die Daten in automatisierten Verfahren verarbeitet, so sind bei der Benachrichtigung die in Absatz 2 Satz 1 Nr. 1 bis 3 genannten Daten mitzuteilen, soweit diese automatisiert gespeichert sind.

(2) Dem Betroffenen ist auf Antrag unentgeltlich Auskunft zu erteilen über

1. die zu seiner Person gespreicherten Daten,
2. den Zweck der Speicherung sowie
3. die Herkunft der Informationen und die Empfänger von Übermittlungen,

auch soweit diese Angaben nicht in einer Datei gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können. Der Betroffene soll die Art der Daten, über die er Auskunft verlangt, näher bezeichnen. Aus Akten ist dem Betroffenen Auskunft zu erteilen, soweit er Angaben macht, die das Auffinden der Daten ermöglichen und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem Auskunftsinteresse des Betroffenen steht. Die Auskunft wird schriftlich erteilt, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

(3) Die Absätze 1 und 2 gelten nicht, soweit

1. die Geschäftszwecke oder Ziele der speichernden Stelle erheblich gefährdet würden und das Inter-

esse des Betroffenen an der Benachrichtigung oder Auskunftserteilung nicht erkennbar überwiegt,

2. die zuständige öffentliche Stelle gegenüber der speichernden Stelle festgestellt hat, daß hierdurch die öffentliche Sicherheit gefährdet oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereitet werden könnten,

3. die personenbezogenen Daten nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen einer dritten Person geheimgehalten werden müssen,

4. die personenbezogenen Daten nicht länger als drei Monate ausschließlich zum Zwecke der Datensicherung gespeichert oder deshalb nach § 35 Abs. 2 Nr. 2 gesperrt sind, weil sie aufgrund gesetzlicher, satzungsgemäßer oder vertraglicher Aufbewahrungsfristen nicht nach § 35 Abs. 4 gelöscht werden dürfen.

§ 35

Berichtigung, Sperrung und Löschung von Daten

(1) Personenbezogene Daten sind unverzüglich zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt,

2. ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist,

3. ihre Verarbeitung unzulässig war und der Betroffene an Stelle der Löschung die Sperrung verlangt,

4. sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

Sind personenbezogene Daten in Akten gespeichert, dann ist die Sperrung nach Satz 1 Nr. 2 nur durchzuführen, wenn die gesamte Akte zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Die Vorschriften über das Verfahren und die Rechtsfolgen der Sperrung gelten entsprechend.

(3) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig war und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen verletzt werden oder wenn es im Falle des Absatzes 2 Nr. 2 der Betroffene verlangt,

2. sie gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse und politische Anschauungen betreffen und die Richtigkeit von der speichernden Stelle nicht bewiesen werden kann und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen verletzt werden,

3. sie strafgerichtliche Verurteilungen betreffen, die nach § 49 des Bundeszentralregistergesetzes einem Verwertungsverbot unterliegen und der Betroffene dies verlangt.

(4) Personenbezogene Daten können gelöscht werden, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen verletzt würden.

(5) Von der Berichtigung gemäß Absatz 1 sowie von der Sperrung gemäß Absatz 2 Nr. 1 und 3 und der Löschung gemäß Absatz 3 sind unverzüglich die Stellen, soweit bekannt, zu verständigen, denen die Daten übermittelt worden sind, es sei denn, daß schutzwürdige Belange des Betroffenen nicht berührt sind.

§ 36

Bestellung eines Beauftragten für den Datenschutz

(1) Die in § 29 Abs. 1 und 2 genannten Personen, Gesellschaften und anderen Personenvereinigungen, die personenbezogene Daten automatisch verarbeiten und hierbei in der Regel mindestens 5 Arbeitnehmer ständig beschäftigen, haben spätestens binnen eines Monats nach Aufnahme ihrer Tätigkeit einen Beauftragten für den Datenschutz schriftlich zu bestellen. Das gleiche gilt, wenn personenbezogene Daten auf andere Weise verarbeitet werden und soweit hierbei in der Regel mindestens 20 Arbeitnehmer ständig beschäftigt sind.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

(3) Der Beauftragte für den Datenschutz ist dem Inhaber, dem Vorstand, dem Geschäftsführer oder dem sonstigen gesetzlich oder verfassungsmäßig berufenen Leiter unmittelbar zu unterstellen. Bestellung und Abberufung bedürfen der Zustimmung des Betriebsrates. Bei der Erfüllung seiner Aufgaben ist der Beauftragte weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Kündigung seines Arbeitsverhältnisses ist einschließlich eines Zeitraumes von einem Jahr nach Beendigung seiner Aufgaben nur aus wichtigem Grund (§ 626 des Bürgerlichen Gesetzbuches) zulässig. Die Kündigung aus wichtigem Grund ist der Aufsichtsbehörde mitzuteilen. Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht von der Verschwiegenheitspflicht durch den Betroffenen befreit wird.

(4) Die zur Bestellung des Beauftragten für den Datenschutz nach Absatz 1 verpflichteten Personen, Gesellschaften und anderen Personenvereinigungen haben dafür zu sorgen, daß der von ihnen bestellte Beauftragte seine Aufgaben erfüllt. Sie haben ihn bei der Erfüllung seiner Aufgaben zu unterstützen; insbeson-

dere sind sie verpflichtet, ihm, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

(5) Dem Beauftragten für den Datenschutz ist die zur Erfüllung seiner Aufgaben erforderliche Fortbildung unter Berücksichtigung der betrieblichen Belange zu ermöglichen. Ist der Beauftragte für den Datenschutz als Arbeitnehmer eingestellt, so ist er für die Zeit der Fortbildung unter Fortentrichtung der Arbeitsvergütung von der Arbeit freizustellen. Die Kosten der Fortbildung trägt der Arbeitgeber. Ist der Beauftragte für den Datenschutz nicht als Arbeitnehmer eingestellt, so ist er für die Zeit der Fortbildung von der Erfüllung der ihm übertragenen Aufgaben freizustellen.

(6) Sein Arbeitsentgelt darf einschließlich eines Zeitraumes von einem Jahr nach Beendigung seiner Aufgaben nicht geringer bemessen werden als das Arbeitsentgelt vergleichbarer Arbeitnehmer mit betriebsüblicher beruflicher Entwicklung. Dies gilt auch für allgemeine Zuwendungen des Arbeitgebers. Soweit nicht zwingende betriebliche Notwendigkeiten entgegenstehen, darf er einschließlich eines Zeitraums von einem Jahr nach Beendigung seiner Aufgaben nur mit Tätigkeiten beschäftigt werden, die den Tätigkeiten der in Satz 2 genannten Arbeitnehmer gleichwertig sind. Zum Zwecke des Arbeitnehmerdatenschutzes arbeitet er mit dem Betriebsrat zusammen; über wichtige Angelegenheiten des Schutzes personenbezogener Daten der Arbeitnehmer hat er den Betriebsrat zu unterrichten. Ohne Einwilligung des Betriebsrates darf er keine Informationen über dessen Tätigkeit an den Arbeitgeber weitergeben.

§ 37

Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz hat die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Schutz personenbezogener Daten sicherzustellen. Zu diesem Zweck kann er sich in Zweifelsfällen an die Aufsichtsbehörde (§ 38) wenden. Er hat insbesondere

1. die Erfüllung der Verpflichtungen der datenverarbeitenden Stelle gemäß § 9 zu überwachen,
2. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen,
3. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Schutz personenbezogener Daten, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenden besonderen Erfordernisse für den Schutz personenbezogener Daten, vertraut zu machen,
4. bei der Auswahl der in der Verarbeitung personenbezogener Daten tätigen Personen beratend mitzuwirken,
5. bei der Entwicklung neuer personenbezogener Datenverarbeitungsanwendungen sowie bei technischen oder organisatorischen Veränderungen in der Datenverarbeitung beratend mitzuwirken,
6. bei der Entscheidung über die Versagung der Auskunft oder der Einsicht gemäß § 34 Abs. 3 mitzuwirken.

(2) Der Beauftragte für den Datenschutz ist über Planungen zum Aufbau automatisierter Datensysteme rechtzeitig zu unterrichten, sofern in dem System personenbezogene Daten verarbeitet werden sollen.

§ 38

Aufsichtsbehörde

(1) Die nach Landesrecht zuständige Aufsichtsbehörde überprüft die Anwendung dieses Gesetzes sowie anderer Vorschriften über den Schutz personenbezogener Daten im Anwendungsbereich dieses Abschnitts, wenn Anhaltspunkte dafür vorliegen, daß gegen eine Rechtsvorschrift über den Schutz personenbezogener Daten verstoßen worden ist. Dies gilt insbesondere, wenn ein Betroffener sich an die Aufsichtsbehörde wendet.

(2) Die Aufsichtsbehörde hat den Beauftragten für den Datenschutz zu unterstützen, wenn er sich an sie wendet (§ 37 Abs. 1 Satz 2). Niemand darf wegen der Anrufung der Aufsichtsbehörde benachteiligt werden.

(3) Die in § 29 Abs. 1 und 2 genannten Personen, Gesellschaften und anderen Personenvereinigungen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Die Sätze 1 und 2 gelten entsprechend für die Empfänger übermittelter personenbezogener Daten.

(4) Die von der Aufsichtsbehörde mit der Überwachung beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, Grundstücke und Geschäftsräume der in Absatz 3 Satz 1 genannten Stellen zu betreten, dort Prüfungen und Besichtigungen vorzunehmen und in die geschäftlichen Unterlagen, namentlich in die nach § 9 zu führenden Dateibeschreibungen und Geräteverzeichnisse, in die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme Einsicht zu nehmen. Der Auskunftspflichtige hat diese Maßnahmen zu dulden. Das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) wird insoweit eingeschränkt.

(5) Die nach Landesrecht zuständige Aufsichtsbehörde kann

1. anordnen, daß Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden,
2. einzelne Verfahren oder den Betrieb einer Datenverarbeitungsanlage untersagen, wenn die von ihr beanstandeten Mängel in angemessener Zeit nicht beseitigt werden,
3. einzelne Verfahren untersagen, die mit den zum Schutz personenbezogener Daten erlassenen Rechtsvorschriften nicht zu vereinbaren sind,
4. die Abberufung des Beauftragten für den Datenschutz verlangen, wenn dieser seine Aufgaben nach § 37 nicht wahrnimmt oder erhebliche Mängel bei der Aufgabenwahrnehmung festgestellt werden.

Die Aufsichtsbehörde unterrichtet in Beschwerdefällen die Beteiligten über das Ergebnis ihrer Überprüfungen. Sie kann darüber hinaus Betroffenen schwerwiegende Verstöße gegen Vorschriften zum Schutz personenbezogener Daten mitteilen, soweit eine Gefährdung der Geschäftszwecke der datenverarbeitenden Stelle nicht zu befürchten ist oder eine solche Gefährdung gegenüber dem berechtigten Informationsinteresse des Betroffenen zurücktreten muß.

(6) Die Anwendung der Gewerbeordnung auf die von den Vorschriften dieses Abschnitts unterliegenden Gewerbebetriebe bleibt unberührt.

(7) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Durchführung des Schutzes personenbezogener Daten im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

(8) Die Länder können Berichte über die Tätigkeit der Aufsichtsbehörden veröffentlichen.

VIERTER ABSCHNITT

Geschäftsmäßige Datenverarbeitung nichtöffentlicher Stellen für fremde Zwecke

§ 39

Anwendungsbereich

(1) Für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts sowie für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, soweit sie die Voraussetzungen von § 10 Abs. 1 Satz 1 oder § 10 Abs. 2 Satz 1 erfüllen, gelten

1. die §§ 40, 42 und 43, soweit diese Stellen geschäftsmäßig geschützte personenbezogene Daten zum Zweck der Übermittlung speichern und übermitteln; dabei ist es unerheblich, ob die Daten vor der Übermittlung verändert werden,
2. die §§ 44 bis 46, soweit diese Stellen Direktwerbung für eigene Zwecke oder geschäftsmäßig für fremde Zwecke betreiben,
3. § 47, soweit diese Stellen geschäftsmäßig geschützte personenbezogene Daten zum Zweck der Übermittlung in anonymisiertem Zustand speichern, sie anonymisieren und so übermitteln,
4. § 48, soweit diese Stellen geschäftsmäßig geschützte personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten.

Für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts gelten außerdem die §§ 49 bis 51; Satz 2 gilt nicht für juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, soweit diese Personen oder Personenvereinigungen geschäftsmäßig geschützte personenbezogene Daten im Auftrag von Behörden oder sonstigen öffentlichen Stellen als Dienstleistungsunternehmen verarbeiten; § 11 Abs. 3 bleibt unberührt.

(2) Die in Absatz 1 genannten Vorschriften gelten für die dort genannten Personen, Gesellschaften und anderen Personenvereinigungen auch insoweit, als die Verarbeitung personenbezogener Daten in deren Auftrag durch andere Personen oder Stellen betrieben wird. In diesen Fällen ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 8 Abs. 1) sorgfältig auszuwählen. § 29 Abs. 2 Satz 3 gilt entsprechend.

§ 40

Datenerhebung, -speicherung, -übermittlung und -nutzung

(1) Das Erheben, das Speichern und die sonstige Nutzung personenbezogener Daten ist zulässig, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Unbeschadet von Satz 1 ist das Speichern in nicht automatisierten Verfahren zulässig, soweit die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen werden.

(2) Die Übermittlung personenbezogener Daten ist zulässig, wenn kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden und der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. Die Gründe für das Vorliegen eines berechtigten Interesses sowie die Mittel für ihre glaubhafte Darlegung sind von der speichernden Stelle und vom Empfänger aufzuzeichnen. § 31 Absätze 3 und 4 gelten entsprechend.

(3) Wird nach einer Datenübermittlung nach Absatz 2 durch den Empfänger eine die Interessen des Betroffenen beeinträchtigende Maßnahme getroffen, so hat der Empfänger dem Betroffenen die übermittelten Daten und die übermittelnde Stelle mitzuteilen.

§ 41

Datenveränderung

Das Verändern personenbezogener Daten ist zulässig, soweit dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

§ 42

Benachrichtigung, Auskunft an den Betroffenen, Einsicht

(1) Werden erstmals zur Person des Betroffenen Daten in Dateien gespeichert, ist er darüber zu benachrichtigen, wenn nicht auf andere Weise sichergestellt worden ist, daß er von der Speicherung eindeutig Kenntnis erlangen konnte. Dabei sind die Art der gespeicherten Daten und die Empfänger regelmäßiger Übermittlungen mitzuteilen. Werden die Daten in automatisierten Verfahren verarbeitet, so sind bei der Benachrichtigung die in Absatz 2 Satz 1 Nr. 1 bis 3 genannten Daten mitzuteilen, soweit diese automatisiert gespeichert sind. Satz 1 gilt nicht für unmittelbar aus allgemein zugänglichen Quellen entnommenen Daten, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, sowie in den Fällen des § 40 Abs. 1 Satz 2.

(2) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck der Speicherung sowie
3. die Herkunft der Daten und die Empfänger von Übermittlungen,

auch soweit diese Angaben nicht in einer Datei gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können. Der Betroffene soll die Art der personenbezogenen Daten, über die er Auskunft verlangt, näher bezeichnen. Aus Akten ist dem Betroffenen Auskunft zu erteilen, soweit er Angaben macht, die das Auffinden der Daten ermöglichen und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem Auskunftsinteresse des Betroffenen steht. Die Auskunft wird schriftlich erteilt, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

(3) § 34 Abs. 3 Nr. 1 bis 3 sowie 4, 1. Alternative, gelten entsprechend.

(4) Die Auskunft ist unentgeltlich. Erfolgt die Datenverarbeitung für fremde Zwecke, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann; im Falle eines Auskunftsbegehrens ist der Betroffene hierauf und ferner darauf hinzuweisen, daß er bei einer näher bezeichneten Stelle unentgeltlich Einsicht in die zu seiner Person gespeicherten Daten nehmen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, daß Informationen unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, daß die Informationen zu berichtigen oder unter der Voraussetzung des § 43 Abs. 3 Nr. 1 zu löschen sind.

§ 43

Berichtigung, Sperrung und Löschung von Daten

(1) Personenbezogene Daten sind unverzüglich zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und weder ihre Richtigkeit noch ihre Unrichtigkeit festgestellt werden kann. Die Vorschriften über das Verfahren und die Rechtsfolgen der Sperrung gemäß § 19 Abs. 2 Satz 2 gelten entsprechend.

(3) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig war und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen verletzt werden,
2. sie gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen betreffen und ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen verletzt werden,
3. sie strafgerichtliche Verurteilungen betreffen, die nach § 49 des Bundeszentralregistergesetzes einem Verwertungsverbot unterliegen und der Betroffene dies verlangt,
4. im übrigen am Ende des dritten Kalenderjahres.

(4) Von der Berichtigung gemäß Absatz 1 sowie von der Sperrung gemäß Absatz 2 und der Löschung gemäß Absatz 3 sind unverzüglich die Stellen, soweit bekannt, zu verständigen, denen die Daten übermittelt worden sind, es sei denn, daß schutzwürdige Belange des Betroffenen nicht berührt werden.

(5) Abweichend von Absatz 1 ist den unmittelbar aus allgemein zugänglichen Quellen entnommenen, zu Dokumentationszwecken gespeicherten Daten auf Verlangen des Betroffenen seine Gegendarstellung für die Dauer der Speicherung dieser Daten beizufügen; die Daten dürfen nicht ohne Gegendarstellung übermittelt werden. Die in Satz 1 genannten Daten sind nicht nach Absatz 2 zu sperren, außer es handelt sich um solche mit dem in Absatz 3 Nr. 2 genannten Inhalt.

§ 44

Datenerhebung und -speicherung zum Zweck der Direktwerbung

(1) Das Erheben und Speichern von personenbezogenen Daten für Zwecke der Direktwerbung ist zulässig, soweit sie

1. unmittelbar aus allgemein zugänglichen Quellen entnommen sind oder
2. aus eigenen vertraglichen, satzungsmäßigen oder sonstigen geschäftlichen Beziehungen stammen oder
3. in zulässiger Weise nach § 45 übermittelt worden sind.

(2) Dient das Erheben bei dem Betroffenen auch Zwecken der Direktwerbung, so ist er hierauf ausdrücklich hinzuweisen. Die Erhebung unter irreführender Zweckangabe ist unzulässig.

§ 45

Datenübermittlung zum Zweck der Direktwerbung

(1) Zum Zweck der Direktwerbung dürfen nur Namen, Titel, akademische Grade, Berufs- oder Amtsbezeichnung, Anschrift und Rufnummer übermittelt werden.

(2) Die Datenübermittlung muß Gegenstand eines schriftlichen Vertrages sein, der die Bedingungen festlegt, zu denen die Daten verwendet werden dürfen.

(3) Die Absicht der Übermittlung muß so bekanntgemacht werden, daß der Betroffene Gelegenheit zur Kenntnisnahme und zum Widerspruch erhält.

(4) Wer personenbezogene Daten zu Zwecken der Direktwerbung Dritten übermittelt, hat aufzuzeichnen, welche Stelle welche Daten nach welchen Auswahlkriterien erhalten hat, und hat die Empfänger darüber zu unterrichten, wenn der Betroffene ein Nutzungsverbot nach § 46 Nr. 1 oder die Löschung nach § 46 Nr. 5 verlangt hat.

§ 46

Rechte des Betroffenen bei der Direktwerbung

Jeder hat das Recht,

1. die Aufnahme seiner Daten in Datensammlungen, die der Direktwerbung dienen, und die Übermittlung zum Zweck der Direktwerbung zu untersagen,
2. von einer werbenden Stelle Auskunft darüber zu verlangen, welche Daten über ihn aus welcher Quelle mit welchen Auswahlkriterien genutzt worden sind,
3. von der speichernden Stelle Auskunft darüber zu verlangen, welche seiner Daten aus welcher Quelle nach welchen Zuordnungsmerkmalen gespeichert sind und welche seiner Daten innerhalb des laufenden und des vorangegangenen Kalenderjahres an wen übermittelt worden sind,
4. die Berichtigung unrichtiger Daten zu verlangen,
5. die Löschung seiner Daten zu verlangen, soweit sie in Datensammlungen gespeichert sind, die der Direktwerbung dienen.

§ 47

Verarbeitung personenbezogener Daten zum Zweck der Übermittlung in anonymisierter Form

(1) Die in § 39 Abs. 1 Satz 1 Nr. 3 genannten Personen, Gesellschaften und anderen Personenvereinigungen sind verpflichtet, die gespeicherten personenbezogenen Daten zu anonymisieren. Die Merkmale, mit deren Hilfe anonymisierte Daten derart verändert werden können, daß sie wieder Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person werden, sind gesondert zu speichern. Diese Merkmale dürfen mit den anonymisierten Daten nicht mehr zusammengeführt werden, es sei denn, daß die dadurch ermöglichte Nutzung der Daten noch für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Für die Nutzung und Löschung personenbezogener Daten gelten §§ 40 und 43 entsprechend.

§ 48

Verarbeitung personenbezogener Daten im Auftrag

Den in § 39 Abs. 1 Satz 1 Nr. 4 genannten Personen, Gesellschaften und anderen Personenvereinigungen ist die Verarbeitung personenbezogener Daten in jeder ihrer in § 2 Abs. 2 genannten Phasen nur im Rahmen der schriftlichen Weisungen des Auftraggebers gestattet.

§ 49

Beauftragter für den Datenschutz

Die in § 40 genannten Personen, Gesellschaften und anderen Personenvereinigungen haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Die Vorschriften der § 36 Abs. 2 bis 4 und § 37 gelten entsprechend.

§ 50

Meldepflichten

(1) Die in § 39 genannten Personen, Gesellschaften und anderen Personenvereinigungen sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen haben die Aufnahme ihrer Tätigkeit bei der zuständigen Aufsichtsbehörde binnen eines Monats anzumelden.

(2) Bei der Anmeldung sind folgende Angaben zu den bei der Aufsichtsbehörde geführten Registern mitzuteilen:

1. Name oder Firma der Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder verfassungsmäßig berufene Leiter

und die mit der Leitung der Datenverarbeitung beauftragten Personen,

3. Anschrift,
4. Geschäftszwecke oder Ziele der Stelle und der Datenverarbeitung,
5. Art der von ihr oder in ihrem Auftrag gespeicherten personenbezogenen Daten,
6. Name des Beauftragten für den Datenschutz.

(3) Bei der Anmeldung sind außerdem noch folgende Angaben mitzuteilen:

1. Art der eingesetzten Anlagen zur automatisierten Datenverarbeitung,
2. bei regelmäßiger Übermittlung personenbezogener Daten, Empfänger und Art der übermittelten Daten.

(4) Absatz 1 gilt für die Beendigung der Tätigkeit sowie die Änderung der nach den Absätzen 2 und 3 mitzuteilenden Angaben entsprechend.

§ 51

Aufsichtsbehörde

Die nach Landesrecht zuständige Aufsichtsbehörde überwacht die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Schutz personenbezogener Daten im Anwendungsbereich dieses Abschnitts. § 38 Abs. 2 bis 8 findet entsprechende Anwendung. Die Aufsichtsbehörde führt das Register über die nach § 50 Abs. 1 anmeldepflichtigen Stellen; das Register kann von jedem eingesehen werden.

FÜNFTER ABSCHNITT

Besondere Vorschriften

§ 52

Datenverarbeitung für wissenschaftliche Zwecke

(1) Zu Zwecken unabhängiger wissenschaftlicher Forschung dürfen personenbezogene Daten für bestimmte Forschungsvorhaben verarbeitet werden, wenn der Betroffene eingewilligt hat. Ohne Einwilligung des Betroffenen dürfen sie nur verarbeitet werden, soweit dessen schutzwürdige Belange, insbesondere wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verarbeitung, nicht beeinträchtigt werden.

(2) Unter den Voraussetzungen des Absatzes 1 Satz 2 dürfen öffentliche und private Stellen personenbezogene Daten ohne Einwilligung des Betroffenen an Stellen mit der Aufgabe unabhängiger wissenschaftlicher Forschung übermitteln. Der Einwilligung des Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Sobald der Forschungszweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungszweck erreicht worden ist. § 12 Abs. 6 findet keine Anwendung.

(4) Die nach Absatz 1 erhobenen oder nach Absatz 2 übermittelten Daten dürfen nur mit Einwilligung der Betroffenen weiterübermittelt oder für einen anderen als den ursprünglichen Zweck verarbeitet oder sonst genutzt werden.

(5) Soweit die weitere Verarbeitung oder Nutzung unzulässig ist, besteht gegenüber Dritten oder Behörden keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, Akten, Dateien oder sonstigen Datenträgern.

(6) Soweit die Vorschriften dieses Gesetzes auf den Empfänger der übermittelten Daten keine Anwendung finden, dürfen personenbezogene Daten nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Absätze 3 und 4 einzuhalten.

(7) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist.

§ 53

Datenverarbeitung der Medien

(1) Für die Verarbeitung personenbezogener Daten durch Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films ausschließlich zu eigenen journalistisch-redaktionellen Zwecken gelten mit Ausnahme der Absätze 2 und 3 und der §§ 7 und 8 die Vorschriften dieses Gesetzes nicht.

(2) Führt die journalistisch-redaktionelle Verwendung personenbezogener Daten zu Gegendarstellungen der Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung in seinen schutzwürdigen Belangen beeinträchtigt, so kann der Betroffene Auskunft über die der Berichterstattung zugrundeliegenden zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann insoweit verweigert werden, als aus den Daten auf die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Der Betroffene kann die Berichtigung unrichtiger Daten oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen.

§ 54

Datenschutzbeauftragter der Rundfunkanstalten des Bundesrechts

(1) Die Rundfunkanstalten des Bundesrechts bestellen jeweils einen Beauftragten für den Datenschutz. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von 4 Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich an den Beauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Verarbeitung oder Nutzung seiner personenbezogenen Daten durch die jeweilige Rundfunkanstalt des Bundesrechts in seinen Rechten verletzt worden zu sein.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der jeweiligen Rundfunkanstalt des Bundesrechts alle zwei Jahre, erstmals zum 1. Januar ..., einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluß eines Organs der jeweiligen Rundfunkanstalt. Die Tätigkeitsberichte übermittelt der Beauftragte für den Datenschutz auch an den Bundesbeauftragten für den Datenschutz.

(5) Weitere Regelungen entsprechend den §§ 23 bis 27 treffen die Rundfunkanstalten des Bundesrechts jeweils für ihren Bereich. § 20 bleibt unberührt.

§ 55

Fernmessen und Fernwirken

(1) Ferngesteuerte Messungen oder Beobachtungen (Fernmeßdienste) in Wohnungen oder Geschäftsräumen dürfen nur vorgenommen werden, wenn der Betroffene zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden ist und nach der Unterrichtung schriftlich eingewilligt hat. Entsprechendes gilt, soweit eine Übertragungseinrichtung dazu dienen soll, in Wohnungen oder Geschäftsräumen andere Wirkungen auszulösen (Fernwirkdienste). Die Einrichtung von Fernmeß- und Fernwirkdiensten ist nur zulässig, wenn der Betroffene erkennen kann, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist. Der Betroffene kann seine Einwilligung jederzeit widerrufen, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Eine Leistung, der Abschluß oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene nach Absatz 1 Satz 1 oder Satz 2 einwilligt. Verweigert oder widerruft er seine Einwilligung, so dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

(3) Soweit im Rahmen von Fernmeß- oder Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Sie sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

§ 56

Video-Überwachung und -Aufzeichnung

(1) Video-Überwachung ist die Beobachtung öffentlichen und privaten Raumes mittels optischer Einrichtungen. Die Bilder werden lediglich laufend übertragen und mittels anderer technischer Geräte (Bildschirm) sichtbar gemacht, nicht jedoch gespeichert. Die Überwachung ist regelmäßig auf eine gewisse Dauer gerichtet und dient Zwecken der Kontrolle oder Sicherung. Die Video-Aufzeichnung ist die Speicherung mittels Video-Überwachung gewonnener Bilder.

(2) Heimliche Video-Überwachung und Video-Aufzeichnung sind unzulässig. Die Video-Überwachung ist zulässig, soweit sie Räume betrifft, für die der Überwachende ein Hausrecht geltend machen kann. Video-Überwachung und Video-Aufzeichnung müssen für die Betroffenen erkennbar sein.

(3) Die Video-Überwachung anderer Räume durch private Stellen ist unzulässig. Die Video-Überwachung anderer Räume als die in Absatz 2 genannten durch öffentliche Stellen ist nur zulässig, soweit dies eine besondere Rechtsvorschrift erlaubt.

(4) Die Video-Aufzeichnung ist zulässig, soweit seitens der speichernden Stelle ein berechtigtes Interesse besteht und schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.

(5) Die Löschung durch Video-Aufzeichnung gewonnener Bilder mit personenbezogenen Daten ist nach 48 Stunden vorzunehmen, es sei denn, eine längere Speicherung ist erforderlich zum Zweck der Beweissicherung für ein Schadensersatz- oder ein Strafverfahren. Soweit die Video-Aufzeichnung nach 48 Stunden zu löschen ist, ist eine Übermittlung der Aufzeichnung ausgeschlossen.

(6) Die durch Video-Überwachung und -Aufzeichnung gewonnenen Daten dürfen nur zweckgebunden verwendet und nicht zur Erstellung von Bewegungsprofilen genutzt werden.

SECHSTER ABSCHNITT

Straf- und Bußgeldvorschriften

§ 57

Straftaten

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, entgegen den Vorschriften dieses Geset-

zes personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, zweckwidrig verwendet, verändert, weitergibt, zum Abruf bereithält oder löscht,
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlaßt,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht. Der Versuch ist strafbar.

(2) Absatz 1 findet nur Anwendung, soweit die Tat nicht nach anderen Vorschriften mit Strafe bedroht ist.

§ 58

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, zweckwidrig verwendet, verändert, weitergibt, zum Abruf bereithält oder löscht,
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlaßt.

Ordnungswidrig handelt auch, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht.

(2) Ordnungswidrig handelt, wer entgegen den Bestimmungen dieses Gesetzes vorsätzlich oder fahrlässig

1. den Betroffenen nicht benachrichtigt,
2. eine vom Betroffenen verlangte Auskunft nicht, nicht richtig oder nicht vollständig erteilt,
3. einen Beauftragten für den Datenschutz nicht oder nicht rechtzeitig bestellt,
4. die in § 40 Abs. 2 Satz 2 bezeichneten Gründe oder Mittel nicht aufzeichnet,
5. die in § 43 Abs. 4 bezeichneten Stellen oder Auswahlkriterien nicht oder nicht vollständig aufzeichnet,
6. die in § 45 Abs. 4 bezeichneten Empfänger nicht unterrichtet,
7. eine Meldung oder Mitteilung nach § 50 nicht, nicht rechtzeitig, nicht richtig oder nicht vollständig vornimmt,
8. einer Anordnung der Aufsichtsbehörde entgegen § 38 Abs. 5 nicht nachgekommen ist,
9. erforderliche technische und organisatorische Maßnahmen nach § 8 nicht oder nicht rechtzeitig vornimmt,
10. entgegen § 16 Abs. 3 oder § 31 Abs. 4 Satz 3 die ihm übermittelten Daten nicht im Rahmen der Zweckbindung verwendet,
11. entgegen § 56 Video-Überwachung und -Aufzeichnung vornimmt, die vorgeschriebene Löschung unterläßt, die durch Video-Überwachung und -Aufzeichnung gewonnenen Daten nicht im Rahmen der Zweckbindung verwendet oder zur Erstellung von Bewegungsprofilen nutzt.

(3) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 100 000 Deutsche Mark geahndet werden.

Artikel 2

Änderung des Verwaltungsverfahrensgesetzes

Das Verwaltungsverfahrensgesetz vom 25. Mai 1976 (BGBl. I S. 1253), geändert durch Artikel 7 Nr. 4 des Gesetzes vom 2. Juli 1976 (BGBl. I S. 1749), wird wie folgt geändert:

1. Nach § 3 wird folgender § 3 a eingefügt:

„§ 3a

Personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse

Die Behörde darf Angaben über persönliche und sachliche Verhältnisse einer natürlichen Person sowie Betriebs- oder Geschäftsgeheimnisse nicht unbefugt offenbaren. Sie unterliegt, soweit sie personenbezogene Daten verarbeitet oder nutzt, den Vorschriften des Bundes-Informationsschutzgesetzes; § 29 bleibt unberührt."

2. § 26 wird wie folgt geändert:
   a) In Absatz 1 Satz 1 werden nach dem Wort „sich" die Wörter „unter Beachtung des § 3a" eingefügt.
   b) In Absatz 2 werden in Satz 3 nach dem Wort „Erscheinen" ein Komma und die Wörter „zur Angabe von personenbezogenen Daten oder von Betriebs- und Geschäftsgeheimnissen" eingefügt; es wird folgender Satz 4 angefügt:

   „Der Auskunftspflichtige kann die Auskunft auf solche Fragen, zu deren Beantwortung er durch Rechtsvorschrift verpflichtet ist, verweigern, soweit die Beantwortung ihn selbst oder einen der in § 383 Abs. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde."
3. § 29 wird wie folgt geändert:
   a) Absatz 2 entfällt.
   b) Absatz 3 wird Absatz 2.
4. § 30 wird aufgehoben.

Artikel 3

Änderung des Gesetzes über das Bundesverfassungsgericht

Das Gesetz über das Bundesverfassungsgericht in der Fassung der Bekanntmachung vom 12. Dezember 1985 (BGBl. I S. 2229) wird wie folgt geändert:

Nach § 13 Nr. 9 wird folgende Nummer 9a eingefügt:

„9a. über die Abberufung des Bundesbeauftragten für den Datenschutz [§ 22 Abs. 5 des Gesetzes zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz — BISG) vom ... in Verbindung mit Artikel 98 Abs. 2 GG],".

Artikel 4

Berlin-Klausel

Dieses Gesetz gilt nach Maßgabe des § 13 Abs. 1 des Dritten Überleitungsgesetzes auch im Land Berlin.

Artikel 5

Inkrafttreten

Dieses Gesetz tritt am ... in Kraft; gleichzeitig tritt das Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz — BDSG) vom 27. Januar 1977 (BGBl. I S. 201) außer Kraft.

Bonn, den 13. Dezember 1988

Wartenberg (Berlin)
Dr. Penner
Dr. Nöbel
Bernrath
Dr. Emmerlich
Graf
Hämmerle
Lambinus
Lutz
Paterna
Schröer (Mülheim)
Dr. Sonntag-Wolgast
Tietjen
Peter (Kassel)
Schütz
Dr. Skarpelis-Sperk
Vahlberg
Weiler
Wiefelspütz
Dr. Vogel und Fraktion

Begründung

A. Allgemeines

Die Datenschutzgesetzgebung bezweckt den Schutz des Bürgers vor Gefahren und den Ausgleich von Schäden, die bei unangemessenem Umgang mit personenbezogenen Informationen entstehen. Anders ausgedrückt bedeutet Datenschutz die Aufgabe, den fairen Umgang mit personenbezogenen Informationen sicherzustellen.

Das Bundesdatenschutzgesetz war in erster Linie als gesetzliche Reaktion auf die stürmische Entwicklung der Informationstechnik gedacht. Mit dem Gesetz wurde die Lösung des Konflikts zwischen dem Informationsbedürfnis von Staat und Gesellschaft einerseits und dem Recht des Bürgers, über seine Daten grundsätzlich selbst zu bestimmen, sein vom Bundesverfassungsgericht in seiner Entscheidung vom 15. Dezember 1983 (Volkszählungsurteil) anerkanntes Recht auf informationelle Selbstbestimmung andererseits angestrebt.

Das Bundesdatenschutzgesetz stellte zum ersten Mal die Verarbeitung von persönlichen Informationen auf eine umfassende Grundlage. Mit der Verabschiedung des Gesetzes im Jahre 1976 wurde gesetzgeberisches Neuland betreten. Vor und nach Erlaß des Gesetzes gab es scharfe Kritik an dem Grundkonzept und an zahlreichen Einzelbestimmungen. Es war allgemeine Meinung, daß das Gesetz schon sehr bald nach Vorliegen der ersten Erfahrungen geändert bzw. ergänzt werden müsse. Dies kam — ungewöhnlich genug — in der abschließenden Lesung im Deutschen Bundestag zum Ausdruck (vgl. 250.Sitzung des Deutschen Bundestages am 10. Juni 1976).

Die Kritik ist seitdem nicht verstummt. Gleichwohl läßt sich heute feststellen, daß sich das Gesetz trotz erkennbar gewordener Schwächen in seinem Grundkonzept bewährt hat.

Initiativen zur Novellierung des Gesetzes setzten bereits in der 8. Legislaturperiode ein. Auch in der 9. und 10. Wahlperiode des Deutschen Bundestages wurden Versuche unternommen, die gebotene Novellierung des Datenschutzgesetzes in Angriff zu nehmen. Diese Bemühungen sind jedoch nicht zum Abschluß gekommen (vgl.Gesetzentwurf der Fraktion der SPD zur Änderung des Bundesdatenschutzgesetzes vom 27. März 1984 — Drucksache 10/1180).

Auch ein Gesetzesantrag der sozialdemokratisch regierten Bundesländer Bremen, Hamburg, Hessen, Nordrhein-Westfalen und Saarland vom 28. Februar 1986 (BR-Drucksache 121/86) verfiel im Bundesrat der Ablehnung durch die unionsregierten Bundesländer.

Das Bundesdatenschutzgesetz ist nunmehr seit fast 11 Jahren in Kraft. Die in dieser Zeit gewonnenen Erfahrungen bei der Anwendung des Gesetzes haben einige erhebliche Mängel deutlich gemacht. Der Bundesbeauftragte für den Datenschutz hat in seinen nunmehr zehn Tätigkeitsberichten die Schwachstellen des Gesetzes überzeugend dargelegt und zahlreiche, gut begründete Änderungsvorschläge gemacht.

Die Novellierungsdiskussion hat einen Stand erreicht, der es ermöglcht und geboten erscheinen läßt, eine umfassende Überprüfung des Bundesdatenschutzgesetzes in Angriff zu nehmen, um das Gesetz den raschen technischen Entwicklungen anzupassen, die zutage getretenen Mängel zu beseitigen und die Rechtsstellung des Bürgers entscheidend zu verbessern.

Die Neufassung des Bundesdatenschutzgestzes ist um so dringlicher geboten, als das Bundesverfassungsgericht in seinem grundlegenden Urteil vom 15. Dezember 1983 (BVerfGE 65, 1ff.) die verfassungsrechtlichen Anforderungen festgestellt hat, denen die Verarbeitung personenbezogener Informationen entsprechen muß.

In den Leitsätzen des Urteils wird dazu ausgeführt:

‚1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Artikels 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen des Rechts auf „informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Neuregelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.‘

In der Zwischenzeit hat das Bundesverfassungsgericht in mehreren Entscheidungen diese Rechtsprechung bekräftigt und ausgebaut. Das Gericht hat z.B. in seinem Beschluß vom 9. März 1988 (1BvL 49/86) darüber hinaus klargestellt, daß das Recht auf informationelle Selbstbestimmung wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten schützt, unabhängig davon, ob die Daten in einer Datei verarbeitet werden.

Das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. Der einzelne muß vielmehr Einschränkungen dieses Rechts im überwiegenden Allgemeininteresse hinnehmen. Solche Beschränkungen bedürfen aber nach Artikel 2 Abs. 1 GG einer den Anforderungen der Normenklarheit entsprechenden gesetzlichen Grundlage und müssen dem Prinzip der Verhältnismäßigkeit genügen. Eine Grundrechtsbeschränkung muß von hinreichenden Gründen des Gemeinwohls gerechtfertigt sein, das gewählte Mittel muß zur Erreichung des Zwecks geeignet und erforderlich sein, und bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe muß die Grenze des Zumutbaren gewahrt sein (vgl. BVerfGE 71, 183 ff.). Daraus folgt, daß gesetzliche Regelungen erforderlich sind, die es im einzelnen ermöglichen, das Selbstbestimmungsrecht über seine Daten wirksam auszuüben. Es bedarf gesetzlicher Festlegungen, unter denen der einzelne Einschränkungen dieses Rechts im überwiegenden Allgemeininteresse hinzunehmen hat.

Diesen verfassungsrechtlichen Anforderungen genügt das geltende Bundesdatenschutzgesetz erkennbar nicht.

Der vorgelegte Entwurf eines Gesetzes zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz — BISG) soll an die Stelle des geltenden Bundesdatenschutzgesetzes treten. Er ist auch ein Beitrag, die wünschenswerte Rechtseinheitlichkeit zwischen Bund und Ländern in diesem Bereich zu erhalten, nachdem die Länder Hessen, Bremen und Nordrhein-Westfalen bereits ihre Landesdatenschutzgesetze im Licht der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz '83 grundlegend novelliert haben. Die Fülle der erforderlichen Gesetzesänderungen läßt eine Neufassung des Gesetzes dringlich geboten erscheinen.

Im Rahmen des vorliegenden Gesetzentwurfs werden in der Sache einheitliche Regelungen für den gesamten Bereich der Informationsverarbeitung durch öffentliche und nicht-öffentliche Stellen erreicht.

Grundsätzlich ist nach dem Volkszählungsurteil des Bundesverfassungsgerichts jeder Umgang der Verwaltung mit personenbezogenen Informationen ohne Rücksicht auf die jeweilige Form als Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu werten. Dieses Grundrecht gilt allgemein, also auch hinsichtlich der nicht-automatisierten Verwaltung personenbezogener Informationen. Dies führt zu einer grundsätzlichen Einbeziehung auch der traditionellen Form der Informationsverarbeitung (Akten) in den Schutzbereich des Gesetzes. Der bisher zentrale Dateibegriff verliert damit an Bedeutung. Die Verarbeitung personenbezogener Informationen aus Akten kann einen viel stärkeren Eingriff darstellen als die automatisierte Verarbeitung. Die unterschiedliche Art der Verarbeitung muß aber bei Auskunfts- und Berichtigungspflichten angemessen berücksichtigt werden. Aus rechtspolitischen Gründen sollte die Regelung über die Informationsverarbeitung in Akten in dieses Gesetz aufgenommen und nicht im Verwaltungsverfahrensgesetz geregelt werden.

Datenschutzrechtliche Sonderregelungen für die Verarbeitung personenbezogener Informationen in oder aus Akten im Verwaltungsverfahrensgesetz sind weder notwendig noch sinnvoll, weil hierdurch die rechtspolitisch wünschenswerte Rechtseinheitlichkeit auf dem Gebiet des Datenschutzes einerseits und dem Gebiet des Verwaltungsverfahrensrechts andererseits ohne Not gefährdet würde.

Den Aussagen des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung kommt auch für die Auslegung der Rechtsbeziehung zwischen Privaten wesentliche Bedeutung zu. Bereiche der Wirtschaft, in denen das informationelle Selbstbestimmungsrecht des einzelnen in besonderer Weise gefährdet erscheint, sollten ohne Rücksicht auf die Art der Datenverarbeitung in den Anwendungs- und Schutzbereich des Gesetzes und in eine umfassende Kontrolle durch die zuständigen Aufsichtsbehörden einbezogen werden. Die zur Wahrnehmung des informationellen Selbstbestimmungsrechts erforderlichen Rechte müssen auch gegenüber Unternehmen der Wirtschaft insgesamt erheblich stärker ausgebaut werden.

Dieser dem Rechtsbewußtsein der Bürger entsprechenden materiell-rechtlichen Datenschutzregelung muß eine ebenso umfaßend angelegte Kontrollbefugnis folgen. Die Rechtsstellung der Kontrollinstanzen für den Datenschutz muß insoweit konsequent verbessert werden. Dem dient insbesondere die Neugestaltung der Institution des Bundesbeauftragten für den Datenschutz, die in Zukunft von einem Selbstkontrollorgan der Exekutive zu einem Hilfs- und Kontrollorgan des Parlaments umgestaltet werden soll. Der Bundesbeauftragte für den Datenschutz soll in Zukunft vom Deutschen Bundestag mit Zweidrittel-Mehrheit gewählt werden. Dies ist ein wesentlicher Beitrag zur Stärkung seiner Unabhängigkeit. Im nicht-öffentlichen Bereich sollen die Befugnisse der Aufsichtsbehörden sowie die Stellung der betrieblichen Datenschutzbeauftragten verstärkt und ausgebaut werden, um auch insoweit den Forderungen des Bundesverfassungsgerichts Rechnung zu tragen, das die besondere Bedeutung einer effektiven Datenschutzkontrolle für die Ausübung des Rechts auf informationelle Selbstbestimmung betont hat.

Die Erhebung personenbezogener Daten muß aus verfassungsrechtlichen Gründen als geschützte Phase der Datenverarbeitung mit ihren jeweiligen Voraussetzungen in den Schutzzweck des Gesetzes einbezogen werden. Gleichzeitig müssen die Aufklärungs- und Belehrungspflichten gegenüber dem Betroffenen praxisnah erweitert werden.

Die Begriffsbestimmungen des Gesetzes sind teilweise neu zu definieren. Ein einheitliches Gesetz für den Schutz personenbezogener Daten für den öffentlichen und den nicht-öffentlichen Bereich kann und sollte beibehalten werden. Die hier übernommene Grundkonzeption des Bundesdatenschutzgesetzes hat sich voll bewährt.

Der Ausgestaltung des Zweckbindungsprinzips kommt bei der Novellierung des Bundesdatenschutzgesetzes grundlegende Bedeutung zu, weil der Bürger bei der Hergabe seiner Informationen darauf ver-

traut oder darauf vertrauen kann, daß diejenigen Umstände, die ihn zur Preisgabe der Informationen veranlaßt haben, auch tatsächlich zutreffen und von der verarbeitenden Stelle beachtet werden. Die Verarbeitung und sonstige Nutzung personenbezogener Informationen ist prinzipiell an den Erhebungszweck zu binden. Eine anderweitige Nutzung im öffentlichen Bereich ist nur unter einzelnen im Gesetz abschließend geregelten Voraussetzungen zulässig.

In Abkehr von den bisher allgemeingehaltenen Übermittlungsvoraussetzungen im öffentlichen Bereich (Informationshilfe/Amtshilfe) soll nur unter enumerativ aufgezählten gesetzlichen Voraussetzungen eine Zweckänderung zulässig sein; den Amtshilfevorschriften des Verwaltungsverfahrensgesetzes soll daher nur noch subsidiäre Bedeutung zukommen.

Die Transparenz der Datenverarbeitung muß durch eine grundsätzliche Anerkennung und teilweise Neugestaltung der Auskunftsrechte des Betroffenen erhöht werden. Das Auskunftsrecht ist im Rahmen des Datenschutzes ein zentrales Recht, das den Betroffenen überhaupt erst in den Stand setzt, seine anderen Datenschutzrechte wahrzunehmen, nämlich der Anspruch darauf zu wissen, wer was wann wo über ihn gespeichert hat. Der Inhalt des Aufkunftsrechts wird auch auf die Herkunft der Daten und die Empfänger regelmäßiger Übermittlungen ausgedehnt. Die Auskunft soll in Zukunft grundsätzlich kostenfrei sein. Dies gilt auch im nicht-öffentlichen Bereich, besonders im Hinblick auf die Direktwerbung, für die besondere Vorschriften vorgesehen sind.

Die Rechtsstellung des Betroffenen soll durch eine Änderung der Vorschriften über die Berichtigung, Sperrung und Löschung von Daten verbessert werden; hierbei werden auch Aspekte des Archivwesens in die gesetzliche Regelung miteinbezogen.

Die Rechtsstellung des Betroffenen wird auch durch die Schaffung eines verschuldensunabhängigen Schadensersatzanspruchs mit einer Haftungsbegrenzung auf 500 000 DM je Schadensfall gestärkt.

Mit dem vorgelegten Gesetzentwurf werden auch Regelungen zur Verarbeitung von Arbeitnehmerdaten im Rahmen des Arbeitsverhältnisses geschaffen.

Die zunehmende Einrichtung von automatisierten Abrufverfahren bedarf einer gesetzlichen Regelung.

Zwecks größerer Wirksamkeit der Selbstkontrolle ist eine Dateibeschreibung für jede Datei vorzusehen. Die Registerführung des Bundesbeauftragten wird auf automatisch geführte Dateien beschränkt.

In einem besonderen Abschnitt werden gesetzliche Regelungen für die Datenverarbeitung für wissenschaftliche Zwecke und die Datenverarbeitung der Medien geschaffen. Nach dem Beispiel der Landesdatenschutzgesetze werden auch für die Rundfunkanstalten des Bundesrechts Datenschutzbeauftragte berufen.

Neueren technischen Entwicklungen sollen die Vorschriften über das Fernmessen und Fernwirken sowie die Video-Überwachung und -Aufzeichnung dienen.

Die Straf- und Bußgeldvorschriften werden gestrafft und deutlicher voneinander abgehoben. Die Vorschrift über die Strafbarkeit erfaßt nur noch den unbefugten Datenumgang in Bereicherungs- oder Schädigungsabsicht. Der Versuch soll in Zukunft strafbar sein.

Alle anderen Verstöße gegen Datenschutzvorschriften werden in Zukunft nur noch als Ordnungswidrigkeit geahndet.

B. Die einzelnen Vorschriften

Zu Artikel 1

Gesetz zum Schutz personenbezogener Informationen

(Bundes-Informationsschutzgesetz — BISG)

Zur Änderung der Gesetzesüberschrift

Die bisherige Überschrift des BDSG (Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung) ist zu eng und überdies mißverständlich. Sie legt den Schluß nahe, als bezwecke das Gesetz den Schutz von Daten vor Mißbrauch bei der Datenverarbeitung. Es geht aber um den Schutz des Bürgers vor Gefahren und den Ausgleich von Schäden, die bei unangemessenem Umgang mit Informationen entstehen. Dem entspricht auch nicht der unglücklich gewählte, gleichwohl eingebürgerte Begriff „Datenschutz". Dieser aus der Welt der Computer entlehnte Begriff stellt zu sehr auf die Technik der Datenspeicherung und -verarbeitung im Computer als einer, gleichwohl wichtigen Art der Informationsverarbeitung ab. Ein „Datum" wird erst durch seine Bedeutung für jemanden zur sinnvollen Nachricht — zur Information. Es geht aber darum, das Informationsverhalten, den fairen Umgang mit personenbezogenen Informationen in der Gesellschaft zu regeln.

Die Überschrift des Gesetzes sollte den Schutzzweck des Gesetzes angemessen wiedergeben, ihn zumindest nicht unangemessen einengen oder verfälschen. Als Titel des Gesetzes wird vorgeschlagen: „Gesetz zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz — BISG). Aus gesetzestechnischen Gründen soll in den Einzelbestimmungen der eingebürgerte Begriff „personenbezogene Daten" als technischer Begriff zunächst beibehalten werden.

Eine solche Neufassung des Gesetzestitels bietet sich auch als Entsprechung zu den gesetzgeberischen Bestrebungen an, die Transparenz der Verwaltung und die Rechtsstellung der Bürger durch ein „Informationszugangs-Gesetz" zu verstärken.

Zu § 1 (Aufgabe und Regelungsbereich des Gesetzes)

Der Wortlaut von § 1 Abs. 1 soll deutlich machen, daß es nicht mehr allein die Aufgabe des Gesetzes sein soll, den Mißbrauch bei der Verarbeitung personenbezogener Daten zu verhindern, sondern daß es

darum geht, grundsätzliche Regelungen für den Gebrauch personenbezogener Daten zu schaffen. In seinem Urteil zum Volkszählungsgesetz '83 hat das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung als Befugnis des einzelnen definiert, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Da diese Beschreibung für den Betroffenen verständlicher ist als der neue Begriff der informationellen Selbstbestimmung, wurde sie bei der Festlegung der Aufgabe des Gesetzes an den Anfang gestellt. Das Bundesverfassungsgericht hat aber auch ausgeführt, daß der einzelne grundsätzlich Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen muß. Das Gericht hat weiter festgestellt, daß diese Beschränkungen „einer gesetzlichen Grundlage bedürfen, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtlichen Gebot der Normenklarheit entspricht". Da auch die Schaffung dieser rechtlichen Grundlage zu der Aufgabe des Gesetzes gehört, wurde sie ebenfalls in § 1 Abs. 1 aufgenommen.

Absatz 2 regelt — wie schon bisher — den Anwendungsbereich des Gesetzes. Danach ist das Gesetz von den dort genannten Behörden und sonstigen Stellen auszuführen. Mit dem Wegfall des nur auf Dateien bezogenen Verarbeitungsbegriffs wird eines der zentralen Anliegen des Entwurfs verwirklicht, nämlich auch die Verarbeitung von personenbezogenen Daten in oder aus Akten zu erfassen. Die Besonderheiten der Aktenführung machen es notwendig, für die Akten in einigen Anwendungsbereichen von den für Dateien geltenden Vorschriften abweichende Regelungen zu treffen.

Absatz 3 regelt die Subsidiarität des Bundes-Informationsschutzgesetzes. Diese Regelung entspricht dem geltenden Recht (§ 45 BDSG).

Zu § 2 (Begriffsbestimmungen)

Die aus dem Gedanken der Selbstbestimmung folgende Befugnis des einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, besteht unabhängig davon, ob die Angaben in Dateien oder Akten gesammelt und weiterverwendet werden. Die Geltung des Gesetzes ist konsequenterweise nicht mehr auf Dateien beschränkt. Die Ausweitung des Anwendungsbereichs dieses Gesetzes auf alle Formen der Datenverarbeitung macht es erforderlich, zusätzlich zu den bisherigen in § 2 aufgeführten Begriffsbestimmungen weitere aufzunehmen.

Beginnend mit der Erhebung als derjenigen Form der Datenverarbeitung, mit der grundsätzlich erstmals das Persönlichkeitsrecht des Betroffenen berührt wird, werden zusätzlich zu den bislang schon geregelten Verarbeitungsformen nunmehr auch das Sperren und das Nutzen erfaßt und beschrieben, wobei durch die Einbeziehung des Nutzens als jeder sonstigen Verwendung sichergestellt ist, daß alle Formen datenschutzrechtlich bedeutsamer Verwendung von Daten dem Anwendungsbereich des Gesetzes zugeführt werden.

In Absatz 3 wurde der Dateibegriff präzisiert und eine mit der Erstreckung der datenschutzrechtlichen Regelungen auch auf die Aktenführung notwendig gewordene Definition des Begriffs „Akte" aufgenommen.

Zu § 3 (Zulässigkeit der Datenverarbeitung und -nutzung)

Die neu gefaßte Vorschrift enthält die allgemeinen Zulässigkeitsvoraussetzungen jeglicher Verarbeitung personenbezogener Daten. Die Vorschrift ist inhaltlich erweitert. Die Aufklärungspflichten verbessern den Schutz des Betroffenen bei freiwilligen Angaben und erleichtern dadurch die Wahrnehmung der Rechte sowie die Entwicklung des Datenschutzbewußtseins.

In Absatz 2 sind im Zusammenhang mit der Umschreibung der Anforderungen an die Einwilligung des Betroffenen nunmehr eindeutige Aufklärungspflichten aufgenommen worden. In Absatz 4 wird bestimmt, unter welchen Voraussetzungen eine Einwilligung unwirksam ist.

Zu § 4 (Automatisiertes Abrufverfahren und regelmäßige Datenübermittlungen)

Das automatisierte Abrufverfahren ist datenschutzrechtlich von besonderer Bedeutung, da die abrufende Stelle über den gesamten Bestand der speichernden Stelle verfügen kann, wenn keine Schranken errichtet werden. Den Verfahren zur automatisierten Direktabfrage von personenbezogenen Daten (On-line-Verfahren) kommt unter den Aspekten des Datenschutzes und der Datensicherung somit besondere Bedeutung zu. Die Regelung für das automatisierte Abrufverfahren gilt sowohl für den öffentlichen wie für den nichtöffentlichen Bereich (Absatz 1). In Absatz 2 werden für den öffentlichen Bereich besondere Voraussetzungen formeller Art, d.h. die Zulassung von On-line-Verfahren nur durch Rechtsvorschriften vorgeschrieben. Absatz 4 enthält das generelle Verbot von On-line-Verfahren aus dem öffentlichen in den privaten Bereich, soweit nicht für jedermann ein Anschluß an Datenbestände offensteht (Absatz 4). Absatz 5 erklärt Absatz 1 und 2 auf regelmäßige Datenübermittlungen für entsprechend anwendbar.

Zu § 5 (Rechte des Betroffenen)

Diese Vorschrift dient der besseren Information der Betroffenen über ihre Rechte. Sie verbessert die Rechtsstellung des Betroffenen. Das Auskunftsrecht ist eines der grundlegenden Datenschutzrechte des Bürgers, das ihn oftmals erst in den Stand versetzt, seine Rechte wirksam geltend zu machen. Es muß den Betroffenen ohne die Belastung mit Gebühren oder Entgelt gewährt werden. Grundsätzlich wird die Ko-

stenfreiheit der Auskunft eingeführt. Der Katalog der Rechte des Betroffenen wird vervollständigt durch das Recht auf Einsicht in die beim Bundesbeauftragten für den Datenschutz und bei den Aufsichtsbehörden geführten Register sowie die Anrufung des Bundesbeauftragten für den Datenschutz bzw. der zuständigen Aufsichtsbehörde.

Absatz 2 legt fest, daß die genannten Rechte nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden können.

Zu § 6 (Schadensersatz)

Durch diese Bestimmung wird ein verschuldensunabhängiger Schadensersatz bei unzulässiger und unrichtiger automatisierter Verarbeitung personenbezogener Daten eingeführt. In schweren Fällen hat der Betroffene auch einen Anspruch auf Ersatz des immateriellen Schadens. Es wird eine Haftungsbegrenzung von 500 000 DM je schädigendes Ereignis vorgesehen.

Absatz 2 regelt die Haftung mehrerer datenverarbeitender Stellen. Nach Absatz 3 haften mehrere Ersatzpflichtige als Gesamtschuldner.

Nach Absatz 4 gelten die Vorschriften des Bürgerlichen Gesetzbuches für das Mitverschulden und die Verjährung des Entschädigungsanspruchs.

Nach Absatz 5 bleiben weitere Ersatzansprüche unberührt.

Nach Absatz 6 ist der Rechtsweg zu den ordentlichen Gerichten eröffnet.

Zu § 7 (Datengeheimnis)

Diese Vorschrift entspricht nach redaktioneller Überarbeitung im wesentlichen dem bisherigen Recht. In Absatz 2 wird allerdings die Verpflichtungserklärung der Mitarbeiter auf Mitarbeiter im nicht-öffentlichen Bereich beschränkt.

Zu § 8 (Technische und organisatorische Maßnahmen)

§ 8 entspricht inhaltlich dem geltenden Recht, wie es in der Anlage zu § 6 BDSG niedergelegt ist. Es hat sich als richtig erwiesen, keine konkreten Maßnahmen für den Einzelfall im Gesetz vorzuschreiben, sondern Sicherungsziele vorzugeben. Die Art und Weise, wie diese zu erreichen sind, richtet sich nach dem jeweiligen Stand der Technik. Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

Absatz 1 und Absatz 2 enthalten die bisherigen „10-Gebote" des Datenschutzes in redaktionell überarbeiteter Fassung.

Absatz 2 soll deutlich machen, daß Datensicherungsmaßnahmen auch bei Akten und nicht-automatisierten Dateien zu treffen sind. Die Verhinderung des Zugriffs durch Unbefugte hat umfassende Bedeutung. Wird ein solcher Zugriff unterbunden, sind auch unbefugte Kenntnisnahme, Veränderung, Löschung sowie das unbefugte Kopieren nicht möglich.

Zu § 9 (Dateibeschreibung)

Die Generalklauseln des Bundesdatenschutzgesetzes haben sich in der Praxis als flexible Auffangvorschriften für die Bereiche, in denen Spezialrecht fehlt, als brauchbar erwiesen. Sie bedürfen jedoch der Konkretisierung bei der Datenverarbeitung durch die datenverarbeitenden Stellen. Ein praktikabler Weg, zu konkreten Festlegungen der Verarbeitungsmodalitäten, insbesondere des Umfangs der Datensammlungen und der zulässigen Zugriffe, zu gelangen, ist die obligatorische Aufstellung von Dateibeschreibungen und Geräteverzeichnissen durch die Betreiber von Datenverarbeitungsanlagen. Die nach geltendem Recht bereits bestehenden Dateiübersichten nach §§ 15 und 19 haben sich als brauchbare Mittel zur Selbstbindung und als Einstieg für die Fremdkontrolle erwiesen. Die Dateibeschreibung ist ferner ein wichtiges Hilfsmittel im Rahmen der Auskunftspflicht. Die Verpflichtung zur Vorhaltung einer Dateibeschreibung gilt nicht für interne nichtautomatisierte Dateien.

Absatz 3 sieht das Vorhalten eines Geräteverzeichnisses vor, das laufend auf dem neuesten Stand zu halten ist. Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates weitere Kriterien festzulegen.

Zu § 10 (Anwendungsbereich)

Die Vorschrift entspricht dem bisherigen Recht.

Zu § 11 (Verarbeitung personenbezogener Daten im Auftrag)

Diese Vorschrift entspricht — redaktionell überarbeitet — dem bisherigen Recht, konkretisiert aber darüber hinaus die Auftragsvergabe und erfordert die konkrete Beschreibung eventuell bestehender Unterauftragsverhältnisse.

Zu § 12 (Datenerhebung)

Mit dieser Vorschrift wird das „Erheben" oder die „Erhebung" als neue Phase der Datenverarbeitung den Vorschriften dieses Gesetzes unterstellt. In § 12 werden die besonderen Voraussetzungen für das Erheben personenbezogener Daten in Ergänzung zu den allgemeinen Zulässigkeitsvoraussetzungen in § 3 umschrieben. In Absatz 1 wird der Grundsatz der Erforderlichkeit gesetzlich verankert. Jede Erhebung ist nur zulässig, wenn das Beschaffen personenbezogener Daten über den Betroffenen zur rechtmäßigen

Aufgabenerfüllung der erhebenden Stelle oder der Stelle, für die die Daten beschafft werden, erforderlich ist.

Nach Absatz 2 dürfen personenbezogene Daten grundsätzlich nur beim Betroffenen mit seiner Kenntnis erhoben werden, da er nur auf diese Weise sein Recht, selbst über die Preisgabe und Verwendung seiner Daten bestimmen zu dürfen, ausüben kann. Die Erhebung bei ihm ohne seine Kenntnis durch Beobachtung sowie die anderweitige Erhebung bei Behörden oder privaten Stellen, muß deshalb die Ausnahme sein.

Nach Absatz 2 Satz 2 darf eine an sich zulässige Datenerhebung nur in einer Art und Weise durchgeführt werden, die das allgemeine Persönlichkeitsrecht des Betroffenen nicht beeinträchtigt. Damit sollen unangemessene und unzumutbare Methoden bei der Erhebung, ebenso aber auch unzumutbare Fragen ausgeschlossen werden.

Absatz 3 schreibt Aufklärungs-, Belehrungs- und Benachrichtigungspflichten fest, die im Rahmen der Erhebung personenbezogener Daten zu beachten sind. Insbesondere ist der Betroffene bei freiwilligen Angaben darauf hinzuweisen, welche möglichen Folgen bei einer Nichtbeantwortung eintreten können.

Absatz 4 regelt in Verbindung mit § 13 Abs. 2 — Zulässigkeit einer Zweckänderung — die Ausnahmefälle, in denen personenbezogene Daten in Abweichung von Absatz 2 bei anderen öffentlichen Stellen erhoben werden dürfen. Der Katalog dieser Voraussetzungen in § 13 Abs. 2 ist abschließend.

Nach Absatz 5 dürfen bei Dritten außerhalb des öffentlichen Bereichs personenbezogene Daten ausnahmsweise ohne Kenntnis des Betroffenen erhoben werden, wenn eine Rechtsvorschrift dies erlaubt oder zwingend voraussetzt, oder wenn der Schutz von Leben oder Gesundheit dies gebietet. Dies wird z.B. der Fall bei Aufnahme medizinisch erforderlicher Daten bei unfall- oder krankheitsbedingter Bewußtlosigkeit des Betroffenen sein.

Nach Absatz 6 ist der Betroffene davon zu benachrichtigen, daß Daten ohne seine Kenntnis erhoben worden sind, sobald die rechtmäßige Erfüllung der Aufgaben dadurch nicht mehr gefährdet wird. Die Benachrichtigung umfaßt die Angabe der Rechtsgrundlage, die Aufklärung über den Zweck der Datenerhebung und bei Übermittlungen auch den Empfänger der Daten.

Zu § 13 (Zweckbindung bei Verarbeitung, Veränderung und sonstiger Nutzung)

§ 13 regelt das die gesamte Datenverarbeitung beherrschende Prinzip der Zweckbindung.

Das Grundrecht auf informationelle Selbstbestimmung vermag seine Wirkung nur zu entfalten, wenn der Verwendungszweck, so wie er sich im Zeitpunkt der Erhebung oder der erstmaligen Speicherung darstellt, grundsätzlich nicht nachträglich geändert wird. Absatz 1 legt diesen Grundsatz fest. Auch für den Fall, daß personenbezogene Daten nicht durch Erhebung anfallen, sondern der öffentlichen Stelle sonstwie zur Kenntnis gelangen, gilt grundsätzlich das Zweckbindungsprinzip. Hier wird an den erstmaligen Akt der Speicherung angeknüpft.

In Absatz 2 sind abschließend die Ausnahmetatbestände definiert, die zur Durchbrechung des Zweckbindungsprinzips berechtigen. Neben der Einwilligung des Betroffenen in Nummer 1 ist eine Verarbeitung für andere Zwecke nach Nummer 2 zulässig, wenn eine Rechtsvorschrift dies erlaubt oder zwingend voraussetzt. Nach Nummer 3 ist eine Durchbrechung des Zweckbindungsprinzips zulässig, wenn hierdurch erhebliche Nachteile für das Gemeinwohl oder eine schwerwiegende Beeinträchtigung der Rechte einzelner verhindert oder beseitigt werden sollen.

Nummer 4 regelt die Durchbrechung im Interesse der Verfolgung von Straftaten und Ordnungswidrigkeiten.

Nummer 5 läßt eine Durchbrechung zu, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, die Verarbeitung im Interesse des Betroffenen liegt und davon ausgegangen werden kann, daß dieser seine Einwiligung erteilt hätte.

Nummer 6 regelt den Fall, daß die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen sind, es sei denn, daß schutzwürdige Belange des Betroffenen offensichtlich entgegenstehen.

Satz 2 stellt klar, daß Daten, die einem besonderen Amts- oder Berufsgeheimnis unterliegen, in erster Linie nach diesen besonderen Regelungen zu behandeln sind.

Absatz 3 regelt für die dort genannten Aufgaben im Wege einer Fiktion, daß die Verwendung personenbezogener Daten im Rahmen dieser Aufgaben als dem ursprünglichen Zweck entsprechend anzusehen ist.

Absatz 4 stellt sicher, daß personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, nicht zu anderen Zwecken verwendet werden dürfen.

Zu § 14 (Datenübermittlung innerhalb des öffentlichen Bereichs)

Abweichend vom geltenden Recht (§ 10 BDSG) ist eine Übermittlung innerhalb des öffentlichen Bereichs nicht bereits dann zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Nunmehr wird sichergestellt, daß eine Übermittlung nur unter den Voraussetzungen des § 13 Abs. 1 oder des § 13 Abs. 2

zulässig ist. Durch diese Vorschrift wird das Zweckbindungsprinzip im Rahmen der Übermittlungsvorschriften verankert. Eine Übermittlung ist ferner zulässig, soweit es zur Entscheidung in einem Verwaltungsverfahren der Beteiligung mehrerer öffentlicher Stellen bedarf.

Absatz 2 enthält Vorschriften über personenbezogene Daten, die einem Berufs- oder besonderem Amtsgeheimnis unterliegen.

Absatz 3 trägt den Besonderheiten der Verarbeitung personenbezogener Daten in und aus Akten Rechnung. Die Besonderheit der Aktenführung ist es, daß in Akten häufig auch personenbezogene Daten einfließen, die nicht zur Aufgabenerfüllung benötigt werden und diese sich zumeist von denen für die Aufgabenerfüllung benötigten Daten nicht trennen lassen. Dieser besonderen Lage wird dadurch Rechnung getragen, daß die Übermittlung auch der nicht zur Aufgabenerfüllung benötigten Daten zulässig ist, sofern nicht berechtigte Interessen des Betroffenen oder eines Dritten an der Geheimhaltung überwiegen. Auf diese Weise übermittelte Daten dürfen jedoch nicht weiter verarbeitet werden.

Absatz 4 regelt die Verantwortlichkeit bei der Übermittlung. Danach trägt die Verantwortung für die Übermittlung die übermittelnde Stelle (das ist die ersuchte Behörde), während die Verantwortung für die Rechtmäßigkeit der mit der Amtshilfe zu verwirklichenden Maßnahme die empfangende Stelle (das ist die ersuchende Behörde) trägt. Der übermittelnden Stelle obliegt es in diesem Fall, die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen. Der Empfänger hat sicherzustellen, daß die Erforderlichkeit der Übermittlung nachträglich überprüft werden kann. Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen. Für den Fall der Übermittlung durch automatisierten Abruf trägt der Empfänger allein die Verantwortung für die Rechtmäßigkeit des Abrufs.

Absatz 5 stellt sicher, daß der Empfänger seinerseits an das Zweckbindungsprinzip gebunden ist. Eine Durchbrechung dieser Zweckbindung durch den Empfänger ist nunmehr wiederum unter den Voraussetzungen des § 13 Abs. 2 zulässig.

Absatz 6 regelt entsprechend die Übermittlung personenbezogener Daten innerhalb einer öffentlichen Stelle. Es soll verhindert werden, daß zwischen den einzelnen Organisationseinheiten einer Behördenorganisation ungehindert personenbezogene Daten hin- und herfließen, obwohl deren Aufgaben unterschiedlich sind und nichts miteinander zu tun haben. Dies schließt eine Übermittlung solcher Daten von einer Verantwortungsebene zur nächst höheren Verantwortungsebene nicht aus.

Zu § 15 (Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften)

Diese Vorschrift übernimmt unverändert das geltende Recht (§ 10 Abs. 2 BDSG).

Zu § 16 (Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs)

§ 16 regelt die Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs. Eine Übermittlung an private Stellen ist nach § 1 nur zulässig, wenn neben dem Erfordernis der rechtmäßigen Aufgabenerfüllung der übermittelnden Stelle das Zweckbindungsgebot des § 13 Abs. 1 nicht durchbrochen wird oder eine Durchbrechung unter den Voraussetzungen des § 13 Abs. 3 nicht vorliegt.

Eine Übermittlung von personenbezogenen Daten an private Stellen ist darüber hinaus nur dann zulässig, wenn sie unter den Voraussetzungen des § 13 Abs. 2 Nr. 1,4 oder 6 für den Zweck verwendet werden dürfen.

Nach Absatz 1 Nr. 3 ist die Übermittlung personenbezogener Daten schließlich auch dann zulässig, wenn der Empfänger ein rechtliches Interesse an den Daten, z.B. im Rahmen von Pfändungs- und Überweisungsbeschlüssen glaubhaft macht und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Durch Absatz 2 soll sichergestellt werden, daß besondere Amts- oder Berufsgeheimnisse, aus denen sich ein Übermittlungsverbot ergibt, zu beachten bleiben.

Absatz 3 verankert den Grundsatz der Zweckbindung auch für diesen Fall der Übermittlung.

Zu § 17 (Datenübermittlung an öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes)

Diese Vorschrift schafft eine Sondervorschrift für Datenübermittlungen an Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatlichen Stellen. Auch hier wird der Zweckbindungsgrundsatz verankert. Durch die Einfügung einer „Ordre-Public-Klausel" soll sichergestellt werden, daß der Betroffene durch die Übermittlung seiner Daten ins Ausland oder außerhalb des Geltungsbereichs des Grundgesetzes nicht schlechter gestellt wird als im Inland, etwa dadurch, daß im Empfängerland gleichwertige Datenschutzvorschriften nicht bestehen.

Zu § 18 (Auskunft an den Betroffenen, Benachrichtigung, Akteneinsicht)

Der Auskunftsanspruch des Betroffenen gehört zu den grundlegenden Datenschutzrechten des Bürgers, da der Betroffene seine übrigen Rechte nur geltend machen kann, wenn er weiß, welche Daten über ihn wo gespeichert sind. Mit der vorgeschlagenen Vorschrift wird die Transparenz der Datenverarbeitung vergrößert und die Rechtstellung des Betroffenen verstärkt. Der Inhalt der Auskunft wird im Gesetz festgeschrieben. Es sind in Zukunft Art der Daten, Zweck und Rechtsgrundlage sowie Herkunft der Daten und die Empfänger von Übermittlungen mitzuteilen.

Dies gilt auch, soweit die Daten nicht zu seiner Person gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können. Der Betroffene soll zur Vereinfachung der Arbeit der Verwaltung die Art der personenbezogenen Daten, über die er Auskunft verlangt, näher bezeichnen.

Beschränkt auf die automatisierte Datenverarbeitung enthält Absatz 2 eine Benachrichtigungspflicht. Die Benachrichtigung enthält die in der Dateibeschreibung gemäß § 9 Abs. 1 Nr. 1 bis 5 festzulegenden Angaben. Der Aufwand, der dadurch der Verwaltung entsteht, hält sich deshalb in vertretbaren Grenzen, weil die ohnehin zu erstellenden Dateibeschreibungen vervielfältigt und an den Betroffenen versandt werden können.

Die besonders weitgehende Art der Unterrichtung rechtfertigt sich dadurch, daß auch das Bundesverfassungsgericht die besondere Schutzbedürftigkeit des Rechts auf informationelle Selbstbestimmung betont hat.
Die Benachrichtigungspflicht bleibt auf automatisierte Dateien beschränkt. Eine Erstreckung auf nicht automatisierte Dateien wäre wegen des damit verbundenen Verwaltungsaufwandes unangemessen. Es würde zudem die Gefahr bestehen, daß es zu einer Flut nicht erbetener Benachrichtigungen der Bürger käme.

Die in Absatz 3 aufgezählten Fälle machen eine Auskunftspflicht entbehrlich, da die Daten einerseits nicht mehr weiter verwendet werden dürfen und die Auskunft andererseits einen erheblichen, unangemessenen Aufwand verursachen würde. Diese Daten werden ausschließlich aus den im Gesetz genannten Gründen gesondert aufbewahrt und lassen sich auch für eine Auskunft an den Betroffenen nicht mehr so leicht erschließen wie Daten, die noch der Verarbeitung unterliegen.

Absatz 4 sieht Sonderregelungen für die Verarbeitung personenbezogener Daten in Akten vor. Diese Sonderregelungen rechtfertigen sich dadurch, daß Akten im Einzelfall schwerer zu finden und auszuwerten sind als Dateien.

Zwar richtet sich auch für Akten das Auskunftsrecht nach den Voraussetzungen des Absatzes 1; wahlweise kann der Betroffene jedoch statt oder neben der Auskunft Akteneinsicht verlangen. Diese Alternativregelung greift damit Überlegungen auf, dem Bürger ein möglichst weites Informationsrecht an seinen eigenen Daten gegenüber der öffentlichen Verwaltung einzuräumen.

Das Auskunfts- und Einsichtsverfahren ist allerdings bei Akten aus Gründen der Verwaltungspraktikabilität (Auffindbarkeit) an die qualifizierten Voraussetzungen des Absatzes 4 Satz 2 gebunden. Der Betroffene muß so konkrete Angaben machen, daß die Daten aufgefunden werden können. Dabei ist das Verhältnismäßigkeitsprinzip zu beachten. Nach Satz 3 ist die Einsichtnahme unzulässig, wenn die Daten des Betroffenen mit Daten Dritter Personen derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich wäre. Für diesen Fall besteht ein Anspruch auf Auskunft.

Absatz 5 regelt die Ausnahmetatbestände von der Auskunft oder der Akteneinsicht. Die Tatbestände in den Nummern 1 bis 3 enthalten solche Beschränkungen des Auskunftsrechts, die der Auskunftsuchende im überwiegenden Gemeinwohlinteresse hinzunehmen hat.

Nach Absatz 6 bedarf die Auskunftsverweigerung grundsätzlich einer Begründung. Wird die Auskunft verweigert und ist eine Offenlegung der Gründe gegenüber dem Betroffenen nicht möglich, so sind die wesentlichen Gründe für diese Entscheidung in einer Weise zu dokumentieren, die eine Nachprüfung durch die zuständigen Stellen — in der Regel durch den Bundesbeauftragten für den Datenschutz — ermöglicht. Deshalb ist der Betroffene für den Fall der Auskunftsverweigerung auf die Möglichkeit hinzuweisen, sich an den Bundesbeauftragten für den Datenschutz zu wenden.

Nach Absatz 7 ist auf Verlangen des Betroffenen dem Bundesbeauftragten für den Datenschutz Auskunft zu erteilen. Dessen Mitteilung an den Betroffenen darf aber keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, soweit die speichernde Stelle nicht einer weitergehenden Auskunft zustimmt.

Zu § 19 (Berichtigung, Sperrung und Löschung von Daten)

Die neu gefaßte Vorschrift über die Berichtigung, Sperrung und Löschung von Daten verbessert die Rechtsposition des Betroffenen unter Beachtung der Besonderheiten der Datenverarbeitung in Akten und der Belange des Archivwesens.

Absatz 1 bleibt gegenüber dem bisherigen Rechtszustand unverändert.

Nach Absatz 2 Nr. 1 sind personenbezogene Daten zu sperren, wenn der Betroffene ihre Richtigkeit bestreitet und sich nicht feststellen läßt, ob sie richtig oder unrichtig sind.

Nach Nummer 2 sind Daten, die nach Absatz 3 grundsätzlich zu löschen wären, zu sperren, wenn Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt würden oder der Betroffene statt der Löschung die Sperrung verlangt.

Nach Nummer 3 sind personenbezogene Daten, die nur zu Zwecken der Datensicherung und der Datenschutzkontrolle gespeichert werden, zu sperren.

Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen. Sie dürfen grundsätzlich nicht mehr verarbeitet oder sonst genutzt werden. Dies ist ausnahmsweise zulässig, wenn die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene in die Nutzung eingewilligt hat.

Absatz 3 regelt die obligatorische Löschung von Daten bei Unzulässigkeit der Datenverarbeitung oder bei Wegfall der Erforderlichkeit zur regelmäßigen Aufgabenerfüllung.

Absatz 4 regelt den Sonderfall der Löschung von Daten in Akten. Unter der Voraussetzung von Satz 1 Nr. 2 ist die Löschung nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist, es sei denn der Betroffene die Löschung verlangt und die weitere Speicherung ihn in unangemessener Weise beeinträchtigen würde. In diesem Falle ist auf Antrag des Betroffenen die Sperrung vorzunehmen.

Absatz 5 schafft eine Archivklausel. Eine Verpflichtung zur Löschung besteht insoweit nicht, soweit Rechtsvorschriften die Übergabe personenbezogener Daten an staatliche oder kommunale Archive anordnen.

Nach Absatz 6 sind über die Berichtigung unrichtiger Daten, die Sperrung bestrittener Daten und die Löschung oder Sperrung unzulässig gespeicherter Daten unverzüglich jene Stellen zu unterrichten, denen die Daten übermittelt worden sind. Ausnahmsweise kann die Unterrichtung unterbleiben bei übermäßigem Aufwand oder wenn nachteilige Folgen für den Betroffenen nicht zu befürchten sind.

Zu § 20 (Durchführung des Datenschutzes in der Bundesverwaltung)

Die Vorschrift wurde gegenüber dem geltenden Recht wesentlich verkürzt, zumal ihr keine konstitutive Bedeutung zukommt.

Zu § 21 (Allgemeine Verwaltungsvorschriften)

Diese Vorschrift ist unverändert aus dem geltenden Bundesdatenschutzgesetz übernommen worden.

Zu §§ 22 bis 28 (Bundesbeauftragter für den Datenschutz)

Die in dem Entwurf eines ... Gesetzes zur Änderung des Grundgesetzes (Artikel 45d — Bundesbeauftragter für den Datenschutz — Drucksache 11/3729) vorgeschlagene Umgestaltung der Institution des Bundesbeauftragten für den Datenschutz zu einem Hilfs- und Kontrollorgan des Deutschen Bundestages, macht die Novellierung der für ihn geltenden gesetzlichen Vorschriften erforderlich.

Zu § 22 (Wahl des Bundesbeauftragten für den Datenschutz)

Nach Absatz 1 wird der Bundesbeauftragte für den Datenschutz — abweichend vom geltenden Recht — in Zukunft vom Deutschen Bundestag gewählt. Seine Amtszeit wird von fünf auf sechs Jahre verlängert. Dies soll eine größere Kontinuität der Amtsführung bewirken. Die einmalige Wiederwahl ist zulässig. Insgesamt zwölf Jahre Amtszeit erscheinen ausreichend; nach einem solchen Zeitraum sollte eine andere Person in das Amt berufen werden, damit neue Initiativen zum Tragen kommen.

Absatz 2 sieht ein Zwei-Drittel-Quorum für die Wahl des Bundesbeauftragten vor. Dies soll gewährleisten, daß sich die Fraktionen über eine unabhängige Person einigen müssen. Als Vorbild dient die Wahl der Verfassungsrichter. Es wird aber bewußt davon abgesehen, einen Wahlausschuß mit der Auswahl zu beauftragen. Der öffentliche Wahlgang im Bundestag bedarf der Rechtfertigung vor der Öffentlichkeit auch dann, wenn — wie es angebracht erscheint — keine Aussprache stattfindet.

Absatz 3 regelt die Verpflichtung durch den Bundespräsidenten. Die Verpflichtungsformel ist der einschlägigen Vorschrift des hessischen Datenschutzgesetzes nachgebildet und löst die nach geltendem Bundesdatenschutzgesetz vorgesehene Eidesleistung ab.

Absatz 4 regelt Beginn und Beendigung des Amtsverhältnisses des Bundesbeauftragten.

Absatz 5 regelt die mögliche Abberufung des Bundesbeauftragten für den Datenschutz durch eine Mehrheit des Deutschen Bundestages. Das dafür vorgesehene Verfahren ist den Vorschriften über die Richterentlassung aus dem Amt nachgebildet.

Absatz 6 enthält für den Verhinderungsfall eine Vertreterregelung.

Zu § 23 (Rechtsstellung des Bundesbeauftragten für den Datenschutz)

Absatz 1 gestaltet die Rechtsstellung des Bundesbeauftragten für den Datenschutz als öffentlich rechtliches Amtsverhältnis aus. Dies betont seine besondere, verfassungsrechtlich herausgehobene Stellung. Aus diesem Grund ist auch die organisatorische Anbindung beim Präsidenten des Deutschen Bundestages geboten. Eine Eingliederung in eines der Bundesministerien wäre mit der Wahl durch den Bundestag nicht vereinbar. Der Bundesbeauftragte für den Datenschutz untersteht der Dienstaufsicht des Präsidenten des Deutschen Bundestages.

Absatz 2 regelt die Personal- und Sachausstattung des Bundesbeauftragten für den Datenschutz. Sie ist im Einzelplan des Deutschen Bundestages in einem eigenen Kapitel auszuweisen.

Absatz 3 regelt die Inkompabilität des Amtes des Bundesbeauftragten mit bestimmten anderen Ämtern, Tätigkeiten und Funktionen. Die Vorschrift entspricht der für den Bundespräsidenten geltenden Regelung des Artikels 55 GG.

Absatz 4 regelt die Besoldung des Bundesbeauftragten. Entsprechend der besoldungsrechtlichen Eingruppierung des Wehrbeauftragten des Deutschen Bundestages ist eine Eingruppierung in die Besoldungsgruppe B 10 (bisher B 9) vorgesehen.

Zu § 24 (Aufgaben des Bundesbeauftragten für den Datenschutz)

Absätze 1 bis 3 regeln die Aufgaben des Bundesbeauftragten. Diese Regelungen entsprechen im wesentlichen dem geltenden Recht. Darüber hinaus wird durch die Einfügung des neuen Absatzes 3 die stärkere Beachtung des Datenschutzes schon bei der Planung neuer Informations- und Kommunikationstechnologien sichergestellt. Dies ermöglicht eine rechtzeitige Beratung und Einflußnahme auf die datenschutzgerechte Ausgestaltung solcher Technologien. Eine solche „Vorverlagerung des Datenschutzes" kann ein wichtiger Beitrag sein, Fehlentwicklungen zu vermeiden und die wünschenswerte Transparenz öffentlicher Planungen in diesem Bereich zu erhöhen.

Es bleibt bei der jährlichen Berichtspflicht. Die bisherige Praxis hat sich bewährt. Die jährliche Vorlage der Berichte und die parlamentarische Diskussion darüber sind ein wichtiger Beitrag, den Stellenwert des Datenschutzes auch im Bewußtsein einer breiten Öffentlichkeit zu verankern.

Absatz 4 konstituiert eine Verpflichtung der Stellen des Bundes, den Bundesbeauftragten zu unterstützen. Insbesondere regelt er das Einsichtsrecht in Unterlagen und Akten und die Verplichtung, dem Bundesbeauftragten jederzeit Zutritt in alle Diensträume zu gewähren.

Der neugeschaffene Absatz 5 soll sicherstellen, daß dem Bundesbeauftragten gesetzliche Geheimhaltungsvorschriften nicht entgegengehalten werden können; andernfalls wäre in den genannten, besonders sensiblen Bereichen eine wirksame, vom Gesetzgeber gewollte Kontrolle der Einhaltung der Datenschutzvorschriften nicht durchführbar.

Absatz 6 regelt, daß die Befugnisse des Bundesbeauftragten von diesem persönlich, aber auch von seinen Beauftragten ausgeübt werden können. Die bisher gegebene Möglichkeit, insbesondere im Sicherheitsbereich auch dem Bundesbeauftragten selbst die Einsicht in Akten und Unterlagen im Einzelfall zu verwehren, entfällt. Das mit der Einrichtung eines Kontrollorgans verfolgte Ziel, eine unabhängige Überprüfung des Datenschutzes im Interesse des Bürgers vor allem dort sicherzustellen, wo diesem selbst wegen vorrangiger Gemeinwohlinterressen keine unmittelbare Kontrollmöglichkeit eingeräumt wird, bliebe andernfalls in einem für den Bürger außerordentlich wichtigen Bereich unerfüllt. Eine Ausnahme wird nur für Einzelfälle zugelassen, in denen personenbezogene Informationen eines Betroffenen, dem eine der genannten Stellen Vertraulichkeit besonders zugesichert hat, betroffen sind.

Die Absätze 7 und 8 regeln die Zusammenarbeit des Bundesbeauftragten für den Datenschutz mit den Landesbeauftragten sowie mit den Aufsichtsbehörden nach §§ 38 und 51 dieses Gesetzes.

Zu § 25 (Verschwiegenheitspflicht)

Diese Vorschrift regelt die Verschwiegenheitspflicht des Bundesbeauftragten. Der Bundesbeauftragte erteilt für sich und seine Beschäftigten Aussagegenehmigungen in eigener Verantwortung.

Diese Vorschrift ist § 23 des hessischen Datenschutzgesetzes nachgebildet worden.

Zu § 26 (Register für automatisiert geführte Dateien)

Die bisherige Vorschrift über das Dateienregister beim Bundesbeauftragten für den Datenschutz (§ 19 Abs. 4 BDSG) ist redaktionell überarbeitet, gestrafft und neu gegliedert worden. Die Vorschrift wird ergänzt durch ein kostenfreies schriftliches Auskunftsrecht und eine jährliche Veröffentlichungspflicht einer Inhaltsübersicht dieses Registers.

Die Einschränkung des Registerinhalts für den Sicherheitsbereich wird aufgehoben, da auch die Kontrolltätigkeit des Bundesbeauftragten für den Datenschutz in diesem Bereich nicht eingeschränkt ist. Die Aufgaben der in Absatz 2 genannten Behörden erfordern — wie nach geltendem Recht — aber eine besondere Behandlung der von ihnen geführten Dateien und die Führung eines besonderen Dateiregisters durch den Bundesbeauftragten für den Datenschutz für die Dateien dieser Behörden, die sich auf eine Übersicht über Art und Verwendungszweck beschränkt und — wie bisher — nicht öffentlich ist.

Zu § 27 (Beanstandungen durch den Bundesbeauftragten für den Datenschutz)

Die Regelung entspricht im wesentlichen dem bisherigen § 20 BDSG. Die neu gefaßte Vorschrift des Absatzes 2 gibt dem Bundesbeauftragten für den Datenschutz die Möglichkeit zu einer flexibleren Handhabung des Instruments der Beanstandung. Er kann künftig auch von einer Beanstandung absehen, wenn die Behebung der Mängel sichergestellt ist. Dieses soll den Behörden einen Anreiz geben, festgestellte Mängel unverzüglich zu beseitigen, um so eine förmliche Beanstandung zu vermeiden.

Der neu eingefügte Absatz 5 regelt den Tatbestand, daß die verantwortliche Stelle es ablehnt, die festgestellten Mängel zu beseitigen (Anrufung der Bundesregierung). Bis zur Entscheidung der Bundesregierung besteht ein Verbot der weiteren Verarbeitung bezüglich der Daten, deren Verarbeitung beanstandet worden ist.

Zu § 28 (Anrufung des Bundesbeauftragten für den Datenschutz)

Absatz 1 enthält nur eine redaktionell angepaßte Fassung der geltenden Vorschrift des § 21 BDSG.

Der neu eingefügte Absatz 2 enthält ein Benachteiligungsverbot für alle Personen, die das Recht der Anrufung in Anspruch nehmen. Beschäftigte des Bundes haben das Recht, sich direkt an den Bundesbeauftragten für den Datenschutz zu wenden, ohne den Dienstweg einzuhalten.

Zu § 29 (Anwendungsbereich)

Diese Vorschrift entspricht im wesentlichen geltendem Recht. In Absatz 2 wird als letzter Satz lediglich die Verpflichtung eingefügt, den Auftrag schriftlich zu erteilen, wobei die Art der Datenverarbeitung, die technisch-organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse konkret zu beschreiben sind.

Zu § 30 (Datenerhebung, -speicherung und -nutzung)

Diese Vorschrift entspricht im wesentlichen § 23 des geltenden Bundesdatenschutzgesetzes. In diese Vorschrift ist aber die Phase der Erhebung einbezogen worden. In Absatz 2 wird der Grundsatz festgelegt, daß Daten grundsätzlich nur beim Betroffenen erhoben werden dürfen. Durch die Art und Weise der Erhebung dürfen schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Absatz 3 postuliert die Geltung des Zweckbindungsprinzips für personenbezogene Daten, die einem Berufs- oder besonderem Amtsgeheimnis unterliegen.

Zu § 31 (Datenübermittlung)

Diese Vorschrift entspricht im wesentlichen § 24 des geltenden Bundesdatenschutzgesetzes. Die Neufassung verankert den Grundsatz der Zweckbindung bei der Übermittlung von Daten. Darüber hinaus enthält sie im neu geschaffenen Absatz 3 eine Art „Bagatellklausel", die die Übermittlung von Daten von geringer Sensibilität zur Erstellung von Listen und Verzeichnissen und zu Zwecken der Werbung und Marktforschung regelt. Die bisherige Regelung hat sich als zu starr erwiesen. Die vorgesehene Erleichterung der Übermittlung in bestimmten Fällen geht aber nicht zu Lasten des Betroffenen. Zu seinen Gunsten schafft Absatz 4 ein Widerspruchsrecht. Darüber hinaus muß die Absicht der Übermittlung von Daten in geeigneter Form dem Betroffenen bekanntgemacht werden, um ihn in den Stand zu setzen, von seinem Widerspruchsrecht Gebrauch zu machen.

Zu § 32 (Datenveränderung)

Diese Vorschrift übernimmt unverändert die Regelung in § 25 des geltenden Bundesdatenschutzgesetzes.

Zu § 33 (Datenverarbeitung im Rahmen des Arbeitsverhältnisses)

Die Einfügung der Vorschrift des § 33 dient dem besonderen Schutz von Arbeitnehmerdaten. Die zulässige Datenverarbeitung ist strikt auf die Erfordernisse der Eingehung, Durchführung, Beendigung und Abwicklung des Arbeitsverhältnisses zu beschränken, soweit nicht andere gesetzliche Vorschriften die Verarbeitung vorschreiben. Weitergehende Nutzungen dürfen weder auf berechtigte Interessen Dritter, noch auf die Einwilligung des Betroffenen gestützt werden, weil die Entschließungsfreiheit des Betroffenen wegen der für ihn existenziellen Bedeutung des Arbeitsverhältnisses faktisch eingeschränkt ist.

Die in den letzten Jahren zu beobachtende rasche Zunahme der Anzahl von Dateien mit Arbeitnehmerdaten zur Nutzung zu den verschiedensten Zwecken (bis hin zu umfassenden Personal- und Management-Informationssystemen) erfordert wegen der damit verbundenen beträchtlichen Gefährdung des Arbeitnehmers dringend gesetzgeberische Maßnahmen. Die zum Teil zwischen den Tarifvertragsparteien bzw. Arbeitnehmern und Arbeitnehmervertretungen abgeschlossenen Tarifverträge und Betriebsvereinbarungen sind nur ein Notbehelf. Sie sind überdies zum Teil unzulänglich. Eine befriedigende Lösung des Problems kann nur in einer gesetzlichen, allgemeine Gültigkeit beanspruchenden Regelung liegen.

Absatz 1 trägt dem Erfordernis der strikten Zweckbindung der Datenverarbeitung zum Arbeitsverhältnis Rechnung. Die Vorschrift stellt zudem sicher, daß die gesetzliche Regelung auch nicht durch sogenannte Datenschutzklauseln unterlaufen werden kann. Die Einwilligung des Betroffenen ist insoweit unwirksam. Besteht ein Personalfragebogen oder ein Arbeitsvertrag, der allgemein für den Betrieb verwendet wird, beschränkt sich die Datenerhebung auf die darin enthaltenen Fragen. Eine Datenübermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwiligung des Betroffenen zulässig.

Absatz 2 enthält eine besondere Regelung zur Erhebung von Angaben vor Abschluß des Arbeitsvertrages. Die nach Satz 1 zulässige Datenerhebung steht in unmittelbarer Beziehung zur Besetzung des Arbeitsplatzes und unterliegt deshalb keiner Beschränkung. Für andere Angaben als berufliche und fachliche Kenntnisse, Erfahrungen und Fähigkeiten verlangt Satz 2 ein berechtigtes Interesse im Hinblick auf die vom Arbeitnehmer zu leistende Arbeit. Da diese Angaben meist nur eine mittelbare Beziehung zu der richtigen Besetzung des Arbeitsplatzes haben, ist ihre Erhebung von dieser einschränkenden Voraussetzung abhängig. Ein berechtigtes Arbeitgeberinteresse an diesen Angaben ist nur dann zu bejahen, wenn die Angaben einen erheblichen Bezug zu der vorgesehenen Arbeitsleistung haben.

Die Absätze 3 und 4 enthalten Sonderregelungen für die Erhebung medizinischer und psychologischer Daten. Dem Arbeitgeber darf in der Regel nur das Ergebnis der Eignungsuntersuchung oder des psychologischen Tests mitgeteilt werden. Derartige Untersuchungen sind nur mit dem Einverständnis des Arbeitnehmers zulässig. Psychologische Tests dürfen nur von Psychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung erhoben werden. Allgemeine Persönlichkeitstests sind nicht zulässig.

Absatz 5 regelt die automatisierte Verarbeitung der Ergebnisse medizinischer und psychologischer Untersuchungen. Arbeitsrechtliche Beurteilungen dürfen nicht allein auf Daten gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

Absatz 6 regelt die Löschung für den Fall, daß ein Arbeitsverhältnis nicht zustandekommt oder nach Beendigung des Arbeitsverhältnisses.

Durch Absatz 7 soll sichergestellt werden, daß die zur Datensicherung zu treffenden Vorkehrungen gemäß § 8 nicht zur Kontrolle von Arbeitnehmern zweckentfremdet werden. Dem Beschäftigten wird ein Auskunftsrecht über die Art dieser Sicherungsdaten eingeräumt.

Zu § 34 (Auskunft an den Betroffenen)

Über die besondere Bedeutung des Auskunftsrechts im Rahmen des Datenschutzes siehe die Begründung zu § 18. Die nach geltendem Recht bestehende Benachrichtigungspflicht (§ 26 BDSG) wird dergestalt erweitert, daß in Zukunft auch die Art der Daten und die Empfänger regelmäßiger Übermittlungen mitzuteilen sind. Werden die Daten in automatisierten Verfahren verarbeitet, sind auch die in Absatz 2 Nr. 1 bis 3 vorgesehenen Angaben (Zweck der Speicherung, Herkunft der Informationen und die Empfänger von Übermittlungen mitzuteilen, soweit diese automatisiert gespeichert sind.

Absatz 2 regelt die grundsätzliche Unentgeltlichkeit der Auskunft.

Die Auskunftspflicht besteht auch, soweit die in Absatz 2 Nr. 1 bis 3 vorgesehenen Daten nicht in einer Datei gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können. Der Betroffene soll geeignete Angaben zum Auffinden seiner Daten machen. Dies gilt auch für die Auskunft in Akten. Dabei ist der Verhältnismäßigkeitsgrundsatz zu beachten.

Die Auskunft wird grundsätzlich schriftlich erteilt, sofern nicht wegen besonderer Umstände eine andere Form angemessen ist.

Absatz 3 regelt die Ausnahmen von der Auskunftspflicht in den Nummern 1 bis 4.

Nummer 1 statuiert eine Ausnahme, falls die Geschäftszwecke oder Ziele der speichernden Stelle erheblich gefährdet würden und das Interesse des Betroffenen an der Benachrichtigung oder Auskunftserteilung nicht erkennbar überwiegt.

Nummer 2: Ausnahme von der Auskunftspflicht aus Gründen des überwiegenden Allgemeininteresses.

Nummer 3 regelt die Ausnahme von der Auskunftspflicht bei gesetzlichen Geheimhaltungspflichten oder wegen überwiegend berechtigte Interessen dritter Personen an einer Geheimhaltung.

Nummer 4 enthält eine Ausnahme für Daten, die lediglich zu Datensicherungszwecken gespeichert werden oder nur deshalb gespeichert sind, weil sie nach gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungsfristen nicht gelöscht werden dürfen.

Zu § 35 (Berichtigung, Sperrung und Löschung von Daten)

Diese neu gefaßte Vorschrift ist entsprechend der Vorschrift in § 19 ausgestaltet und verstärkt die Rechtsstellung des Betroffenen.

Absatz 1 entspricht geltendem Recht.

Absatz 2 regelt die Voraussetzungen des Sperrungsanspruchs.

Satz 2 regelt den Sonderfall der Speicherung von Daten in Akten.

Absatz 3 regelt die Voraussetzungen des Löschungsanspruchs.

Nummer 2 regelt besondere Daten, deren Richtigkeit von der speichernden Stelle nicht bewiesen werden kann und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange der Betroffenen verletzt werden.

Nummer 3 regelt strafrechtliche Verurteilungen, die einem Verwertungsverbot unterliegen.

Absatz 4 ermächtigt zur Löschung von Daten bei Wegfall der Erforderlichkeit zur Zweckerfüllung.

Absatz 5 regelt die Benachrichtigung von Stellen, denen die Daten übermittelt worden sind, es sei denn, daß schützwürdige Belange des Betroffenen nicht berührt sind.

Zu § 36 (Bestellung eines Beauftragten für den Datenschutz)

Diese Vorschrift übernimmt im wesentlichen § 28 des geltenden Bundesdatenschutzgesetzes. Bestellung und Abberufung des Datenschutzbeauftragten werden aber an die Zustimmung des Betriebsrates geknüpft. Es werden verschärfte Vorschriften über den Kündigungsschutz eingeführt. Die Kündigung ist in Zukunft nur aus wichtigem Grund (§ 626 BGB) zulässig. In Absatz 4 wird über die bisher geltende allgemeine Verpflichtung der datenverarbeitenden Stelle hinaus, den Beauftragten für den Datenschutz zu unterstützen, die besondere Verpflichtung eingeführt, ihm Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

Absatz 5 stellt eine Vorschrift über die Fortbildung des Beauftragten dar. Sie ist der einschlägigen Vorschrift

des Gesetzes über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit vom 12. Dezember 1973 (BGBl. I S. 1885) nachgebildet.

Absatz 6 enthält Vorschriften über sein Arbeitsentgelt und seine Beschäftigung nach Beendigung seiner Tätigkeit. Er enthält darüber hinaus eine Verpflichtung des Datenschutzbeauftragten, zu Zwecken des Arbeitnehmerdatenschutzes mit dem Betriebsrat zusammenzuarbeiten. Insoweit unterliegt er der Verschwiegenheit gegenüber dem Arbeitgeber.

Zu § 37 (Aufgaben des Beauftragten für den Datenschutz)

Diese Vorschrift entspricht im wesentlichen § 29 des geltenden Bundesdatenschutzgesetzes in redaktioneller Überarbeitung. Nach dieser Vorschrift ist eine möglichst frühzeitige Beteiligung des Betriebsbeauftragten bei der Entwicklung neuer personenbezogener Datenverarbeitungsanwendungen sowie bei technischen und organisatorischen Veränderungen der Datenverarbeitung vorgesehen. Er hat erweiterte Beratungs- und Mitwirkungspflichten.

Zu § 38 (Aufsichtsbehörde)

Durch die Neufassung der Vorschrift wird die Rechtsstellung der Aufsichtsbehörde im nicht-öffentlichen Bereich gestärkt. In Absatz 1 werden zunächst die Befugnisse der Aufsichtsbehörde insofern erheblich erweitert, als sie nunmehr von sich aus, also ohne auf eine Beschwerde von außen angewiesen zu sein (sog. „Anlaßaufsicht"), im Einzelfall Überprüfungen vornehmen kann, nämlich dann, wenn sonstige Anhaltspunkte für einen Gesetzesverstoß vorliegen. In Absatz 2 wird ein gesetzliches Benachteiligungsverbot für alle eingeführt, die sich an die Aufsichtsbehörde wenden. In Absatz 5 werden die Sanktionsmöglichkeiten der Aufsichtsbehörde bis hin zur Stillegung der Datenverarbeitungsanlage maßgeblich verstärkt. Der Aufsichtsbehörde wird im übrigen das Recht eingeräumt, die Abberufung eines Beauftragten für den Datenschutz zu verlangen, wenn dieser seine Aufgaben nicht wahrnimmt. In Absatz 8 werden die Länder ermächtigt, in geeigneter Form einen Bericht über die Tätigkeit der Aufsichtsbehörden zu veröffentlichen. Dies schafft mehr Transparenz, ermöglicht es, neue technische Entwicklungen und Probleme rechtzeitig zu erkennen und ggf. erforderlich werdende gesetzliche Maßnahmen „vorsorgend" auch in diesem Bereich in Angriff zu nehmen. In einigen Bundesländern ist dies bereits Praxis.

Zu § 39 (Anwendungsbereich)

Diese Vorschrift entspricht nach redaktioneller Überarbeitung im wesentlichen § 31 des geltenden Bundesdatenschutzgesetzes.

Zu § 40 (Datenerhebung, -speicherung, -übermittlung und -nutzung)

Absatz 1 regelt die Zulässigkeitsvoraussetzung des Erhebens, Speicherns oder der sonstigen Nutzung personenbezogener Daten nicht-öffentlicher Stellen für fremde Zwecke. In nicht automatisierten Verfahren ist das speichern zulässig, wenn die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen wurden.

Absatz 2 regelt die Übermittlung. Der Empfänger muß ein berechtigtes Interesse an der Kenntnis glaubhaft dargelegt haben. Die Gründe sind aufzuzeichnen. Die in § 31 Abs. 3 aufgeführten Daten können unter erleichterten Bedingungen übermittelt werden. Für diese Daten gelten § 31 Abs. 3 und 4 entsprechend.

Nach Absatz 3 hat der Empfänger der übermittelten Daten den Betroffenen über die Daten und die übermittelnde Stelle zu unterrichten, falls der Empfänger eine die Interessen des Betroffenen beeinträchtigende Maßnahme trifft. Diese Regelung verstärkt die Rechtsstellung des Betroffenen, sie setzt ihn in Stand, ggf. unrichtige Daten zu berichtigen.

Zu § 41 (Datenveränderung)

Diese Vorschrift entspricht § 33 des geltenden Bundesdatenschutzgesetzes.

Zu § 42 (Benachrichtigung, Auskunft an den Betroffenen, Einsicht)

Diese Vorschrift regelt das Auskunftsrecht im Vierten Abschnitt des Gesetzes (geschäftsmäßige Datenverarbeitung nicht-öffentlicher Stellen für fremde Zwecke).

Entsprechend den Vorschriften in §§ 18 und 34 des Entwurfs werden die Auskunftspflichten zugunsten des Betroffenen gestärkt.

Werden erstmals zur Person des Betroffenen Daten in Dateien gespeichert, ist er darüber zu benachrichtigen. Dabei sind Art der Daten und Empfänger regelmäßiger Übermittlungen mitzuteilen. Werden die Daten in automatisierten Verfahren verarbeitet, so erstreckt sich die Auskunftspflicht auch auf den Zweck der Speicherung, Herkunft der Daten und die Empfänger der Übermittlungen, soweit diese automatisiert gespeichert sind.

Diese Bestimmung des Satzes 1 gilt nicht für unmittelbar aus allgemein zugänglichen Quellen entnommene Daten, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben (Verzeichnisse von Vereinsmitgliedern etc.) sowie auf alle Daten, die nach § 4o Absatz 1 Satz 2 aus allgemein zugänglichen Quellen stammen.

Absatz 2 regelt den Umfang der Auskunftspflicht. Der Auskunftsanspruch besteht auch, soweit die Daten in Absatz 2 Nr. 1 bis 3 nicht in einer Datei gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können. Der Betroffene soll geeignete Angaben

zur Erleichterung des Auffindens dieser Daten machen. Der Auskunftsanspruch gilt auch für die Auskunft aus Akten. Dabei ist der Verhältnismäßigkeitsgrundsatz zu beachten. Die Auskunft wird schriftlich erteilt, sofern nicht wegen besonderer Umstände eine andere Form angemessen ist.

Absatz 3 verweist auf die Ausnahmen von der Auskunftspflicht in § 34 Abs. 3 Nr. 1 bis 3 sowie 4, 1. Alternative.

Nach Absatz 4 ist auch im Bereich der geschäftsmäßigen Datenverarbeitung nicht-öffentlicher Stellen für fremde Zwecke die Auskunft grundsätzlich unentgeltlich. Zugunsten der Kreditschutzorganisationen wird eine Ausnahmeregelung geschaffen, nach der ein Entgelt verlangt werden darf, wenn der Betroffene die Auskunft gegenüber Dritten zu eigenen wirtschaftlichen Zwecken nutzen kann. In diesem Fall steht dem Betroffenen aber alternativ ein unentgeltliches Einsichtsrecht in die zu seiner Person gespeicherten Daten zu. Der Betroffene ist darauf hinzuweisen, und es ist ihm die entsprechende Stelle zur Einsichtnahme näher zu bezeichnen.

Hinsichtlich der Höhe des Entgelts bleibt es bei der Regelung im geltenden Recht. Dies gilt auch für den Wegfall der Entgeltlichkeit, wenn besondere Umstände die Annahme rechtfertigen, daß Informationen unrichtig oder unzulässig gespeichert worden sind, oder in dem die Auskunft ergibt, daß die Information zu berichtigen oder unter den Voraussetzungen des § 43 Abs. 3 Nr. 1 zu löschen sind.

Zu § 43 (Berichtigung, Sperrung und Löschung von Daten)

Diese Vorschrift ist entsprechend den Vorschriften des § 19 und des § 35 neu gefaßt worden und verstärkt die Rechtsstellung des Betroffenen.

Nach Absatz 3 Nr. 4 sind über die Löschungsgründe im Dritten Abschnitt des Gesetzes hinaus, im Vierten Abschnitt die Daten am Ende des 3. Kalenderjahres zu löschen.

Absatz 4 enthält die übliche Benachrichtigungspflicht an Stellen, denen die Daten übermittelt worden sind.

Absatz 5 enthält abweichend von Absatz 1 für unmittelbar aus allgemein zugänglichen Quellen entnommener, zu Dokumentationszwecken gespeicherte Daten eine Sonderregelung. Der Betroffene kann aber durch die Beifügung einer Gegendarstellung für die Dauer der Speicherung dieser Daten verlangen. Die Daten dürfen nicht ohne Gegendarstellung übermittelt werden. Diese Daten sind grundsätzlich auch nicht zu sperren, außer es handelt sich um Daten mit dem in Absatz 3 Nr. 2 genannten Inhalt (gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse und politische Anschauungen), deren Richtigkeit von der speichernden Stelle nicht bewiesen werden kann.

Zu § 44 (Datenerhebung und -speicherung zum Zweck der Direktwerbung)

Zu § 45 (Datenübermittlung zum Zweck der Direktwerbung)

Zu § 46 (Rechte des Betroffenen bei der Direktwerbung)

In den §§ 44, 45 und 46 sind Sondervorschriften für die besondere Problematik der Datennutzung zu Zwekken der sog. Direktwerbung enthalten. Diese Werbungsform stößt auf kritische Resonanz bei den Betroffenen. Mit diesen Vorschriften soll der Datenschutz bei dieser Form der wirtschaftlichen Betätigung für alle Beteiligten eindeutig geregelt werden. § 44 enthält die Zulassungsvoraussetzungen für das Erheben und Speichern von personenbezogenen Daten für Zwecke der Direktwerbung. Der Betroffene, dessen Daten auch zu Zwecken der Direktwerbung dienen, ist darauf hinzuweisen; die Erhebung unter irreführender Zweckangabe ist unzulässig.

§ 45 enthält eine Vorschrift über die Datenübermittlung zum Zweck der Direktwerbung. Hier dürfen bestimmte listenmäßige Auskünfte übermittelt werden. Der Betroffene muß Gelegenheit zur Kenntnisnahme und zum Widerspruch haben. Wer Daten zu Zwecken der Direktwerbung übermittelt, hat aufzuzeichnen, welche Stellen, welche Daten nach welchen Auswahlkriterien erhalten haben und hat die Empfänger darüber zu unterrichten, wenn der Betroffene ein Nutzungsverbot nach § 46 Nr. 1 oder die Löschung nach § 46 Nr. 5 verlangt hat.

§ 46 regelt die Rechte des Betroffenen bei der Direktwerbung. Ihm wird ein Recht zum Widerspruch eingeräumt. Er hat ein Auskunftsrecht, er hat ein Berichtigungsrecht bei unrichtigen Daten und er hat ein Löschungsrecht.

Zu § 47 (Verarbeitung personenbezogener Daten zum Zweck der Übermittlung in anonymisierter Form)

Diese Vorschrift entspricht — nach redaktioneller Überarbeitung — im wesentlichen § 36 des geltenden Bundesdatenschutzgesetzes.

Zu § 48 (Verarbeitung personenbezogener Daten im Auftrag)

Diese Vorschrift übernimmt § 37 des geltenden Bundesdatenschutzgesetzes, allerdings nunmehr unter Einbeziehung auch der Erhebungsphase. Zudem ist in Zukunft eine schriftliche Weisung des Auftraggebers erforderlich.

Zu § 49 (Beauftragter für den Datenschutz)

Diese Vorschrift entspricht § 38 des geltenden Bundesdatenschutzgesetzes.

Zu § 50 (Meldepflichten)

Diese Vorschrift übernimmt im wesentlichen § 39 des geltenden Bundesdatenschutzgesetzes. Der Pflichtenkatalog wird durch die Verpflichtung zur Anmeldung der Art der eingesetzten Anlagen zur automatisierten Datenverarbeitung erweitert.

Zu § 51 (Aufsichtsbehörde)

Diese Vorschrift übernimmt unter redaktioneller Anpassung § 40 des geltenden Bundesdatenschutzgesetzes.

Zu § 52 (Datenverarbeitung für wissenschaftliche Zwecke)

Die Verarbeitung personenbezogener Daten zu Zwecken wissenschaftlicher Forschung bedarf der gesetzlichen Regelung, um das Spannungsverhältnis zwischen Forschung und informationellem Selbstbestimmungsrecht sachgerecht aufzulösen. Die bisher bestehenden berufsethischen Vorschriften und Selbstkontrollmechanismen haben sich nicht als ausreichend erwiesen und zu großer Unsicherheit geführt.

Absatz 1 fordert grundsätzlich die Einwilligung des Betroffenen; ohne dessen Einwilligung darf die Datenverarbeitung nur stattfinden, wenn dessen schutzwürdige Belange nicht berührt werden. Indizien dafür sind insbesondere die Art oder Offenkundigkeit der Daten oder die Art der Verarbeitung.

Absatz 2 regelt die Zulässigkeit der Übermittlung an öffentliche und private Stellen, die unabhängige wissenschaftliche Forschung durchführen. Sie ist ohne Einwilligung nur unter den Voraussetzungen des Absatzes 1 Satz 2 zulässig. Sie ist darüber hinaus bei erheblichem Überwiegen des öffentlichen Interesses an der Durchführung des Forschungsvorhabens und nur dann zulässig, wenn der Zweck nicht auf andere Weise oder nur mit unverhältnismäßig hohem Aufwand erreicht werden kann.

Absatz 3 regelt die möglichst rasche gesonderte Speicherung der Merkmale, mit denen ein Personenbezug hergestellt werden. Diese Vorschrift soll einer möglichen Deanonymisierung vorbeugen. Diese Daten sind nach Erreichung des Forschungsvorhabens zu löschen.

Absatz 4 macht die Weiterübermittlung oder Änderung der Zweckbindung von der Einwilligung des Betroffenen abhängig.

Absatz 5 soll die im Rahmen wissenschaftlicher Forschung zulässigerweise erhobenen Daten vor dem Zugriff Dritter oder Behörden schützen. Insoweit besteht keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Vorlage oder Auslieferung von vorhandenen Materialien.

Absatz 6 erstreckt den Schutz auf Empfänger außerhalb des Geltungsbereichs dieses Gesetzes. Die Übermittlung wird von der Verpflichtung des Empfängers abhängig gemacht, die Vorschriften der Absätze 3 und 4 einzuhalten.

Absatz 7 trifft eine neue Regelung über die Befugnisse zur Veröffentlichung personenbezogener Daten im Rahmen wissenschaftlicher Forschung. Die Veröffentlichung ist nur zulässig, wenn der Betroffene eingewilligt hat, oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist. Hier solll das informationelle Selbstbestimmungsrecht gegenüber dem zeitgeschichtlichen Interesse zurücktreten.

Zu § 53 (Datenverarbeitung der Medien)

Für die Datenverarbeitung der Medien wird eine Sonderbestimmung eingeführt. Die allgemeine Gültigkeit beanspruchenden Bestimmungen des Datenschutzgesetzes können nicht unverändert für die Medien gelten, insbesondere nicht die Vorschriften über die Aufsicht des Staates. Die Medienfreiheit ist für ein demokratisches Gemeinwesen von grundlegender Bedeutung; die Rechte des Betroffenen dürfen aber auch gegenüber Presse, Rundfunk und Fernsehen nicht vernachlässigt werden. Die Archive der Medien, die zunehmend auf automatisierte Verfahren umgestellt werden, enthalten so brisantes Material, daß besondere rechtliche Schutzbestimmungen erforderlich sind. Die in der Rechtsprechung bisher entwickelten Grundsätze des allgemeinen Persönlichkeitsrechts reichen nicht aus. Die Vorschrift ist einer entsprechenden Bestimmung des Entwurfs eines Presserechtsrahmengesetzes vom 25. Juli 1974 nachgebildet.

Den Betroffenen werden Rechte auf

- Speicherung einer Gegendarstellung in angemessenem Umgang im Archiv,
- Auskunft über personenbezogene Daten, und für den Fall der Unrichtigkeit
- Berichtigung

eingeräumt.

Zu § 54 (Datenschutzbeauftragter der Rundfunkanstalten des Bundesrechts)

Entsprechend den einschlägigen Vorschriften in den Landesdatenschutzgesetzen für die Rundfunkanstalten wird auf Bundesebene für die Rundfunkanstalten des Bundesrechts jeweils ein Beauftragter für den Datenschutz eingeführt. Seine Stellung ist der des Bundesbeauftragten für den Datenschutz angeglichen.

Absatz 5 berücksichtigt die aus Artikel 5 Abs. 1 GG folgende Staatsfreiheit der Rundfunkanstalten. Die Rundfunkanstalten haben die Möglichkeit, die Einzelheiten der Amtsführung des Datenschutzbeauf-

tragten unter Berücksichtigung der rundfunkspezifischen Besonderheiten selbst zu regeln.

Zu § 55 (Fernmessen und Fernwirken)

Die neue Vorschrift trifft erstmals generelle Bestimmungen über die Zulässigkeit der Einrichtung von Fernmeß- und Fernwirkdiensten. Dieser erhebliche Eingriff in das informationelle Selbstbestimmungsrecht ist nach Absätzen 1 und 2 nur zulässig, wenn der Betroffene nach einer im einzelnen vorgeschriebenen Unterrichtung durch die einrichtende Stelle seine Einwilligung schriftlich erklärt hat. Der Betreffende muß ferner erkennen können, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist. Im Zweifel gilt das Abschalten des Dienstes als Widerruf.

Nach Absatz 2 besteht ein Junktimverbot, die vertragliche Leistung, den Abschluß oder die Abwicklung des Vertragsverhältnisses von der Einwilligung des Betroffenen zur Einrichtung der Dienste abhängig zu machen. Damit soll die Entscheidungsfreiheit des Betroffenen soweit wie möglich gewahrt bleiben. Ihm dürfen nur die unmittelbaren Kosten der Verweigerung oder des Widerrufs treffen (Nachteilsverbot). Nach Absatz 3 gilt strenge Zweckbindung bei der Verarbeitung personenbezogener Daten und ein obligatorisches Löschungsgebot.

Zu § 56 (Video-Überwachung und -Aufzeichnung)

Der zunehmende Einsatz der Videotechnik zur Beobachtung öffentlichen und privaten Raums (Beobachtung von Verkehrsflächen wie Bahnsteigen, Bahnhofshallen, Verkehrsebenen, Sicherung von Schalterräumen in Banken etc.) kommt in bezug auf das Grundrecht der freien Entfaltung der Persönlichkeit große Bedeutung zu. Die rechtliche Regelung dieser neuen Technik erscheint dringend geboten.

Absatz 1 enthält die Begriffsbestimmungen der „Videoüberwachung" und der „Video-Aufzeichnung".

Absatz 2 enthält ein grundsätzliches Verbot der heimlichen Anwendung dieser Technik. Die Einführung der Video-Überwachung ist abhängig vom Bestehen eines Hausrechts. Die Anwendung dieser Technik muß für den Betroffenen erkennbar sein.

Absatz 3 läßt ausnahmsweise die Video-Überwachung durch öffentliche Stellen zu, soweit dies eine besondere Rechtsvorschrift erlaubt.

Absatz 4 enthält die allgemeinen Voraussetzungen für die Zulässigkeit der Video-Aufzeichnung.

Absatz 5 enthält Regeln über die Löschung der aufgezeichneten Daten sowie ein Übermittlungsverbot, um die Umgehung der Löschungsverpflichtung zu verhindern.

Absatz 6 regelt die Zweckbindung und enthält ein Verbot, die durch Video-Überwachung und -Aufzeichnung gewonnen Daten zur Erstellung von Bewegungsprofilen zu nutzen.

Zu § 57 (Straftaten) und **§ 58** (Ordnungswidrigkeiten)

Die Straf- und Ordnungswidrigkeitsvorschriften werden neu geordnet. Damit ist auch ein Effekt der „Entkriminalisierung" verbunden. Fehlverhalten im Zusammenhang mit der Verarbeitung personenbezogener Daten, unabhängig davon, ob es sich um eine Datei oder nichtdateimäßige Verarbeitung handelt, ist nach Absatz 1 nur dann strafbewehrt, wenn es sich um ein qualifiziertes Delikt handelt, der Täter also in Bereicherungs- oder Schädigungsabsicht vorgeht. Die in Absatz 1 Nr. 1 und 2 sowie in Absatz 2 aufgeführten Tatbestände sind den neuen Regelungen dieses Gesetzes angepaßt. Die Strafandrohung entspricht der bisherigen Höhe in § 33 Abs. 2 des geltenden Bundesdatenschutzgesetzes. In Zukunft soll aber auch der Versuch strafbar sein. Die neue Vorschrift ist als Offizialdelikt ausgestaltet.

Der Ordnungswidrigkeitenkatalog ist überarbeitet und ergänzt worden.

Zu Artikel 2

Gesetz zur Änderung des Verwaltungsverfahrensgesetzes

Im Hinblick auf das Gesamtkonzept zur Änderung des Bundesdatenschutzgesetzes und des Verwaltungsverfahrensgesetzes sind in das Verwaltungsverfahrensgesetz einige Klarstellungen aufzunehmen, aus denen sich die Geltung des Bundes-Informationsschutzgesetzes auch auf den Bereich des Verwaltungsverfahrens unzweifelhaft ergibt.

Zu Artikel 3

Gesetz zur Änderung des Gesetzes über das Bundesverfassungsgericht

Dies ist eine Folgeänderung, die sich aus § 22 Abs. 5 des Bundes-Informationsschutzgesetzes ergibt. Danach kann der Bundestag mit der Mehrheit seiner Mitglieder beim Bundesverfassungsgericht die Abberufung des Bundesbeauftragten für den Datenschutz aus den Gründen beantragen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Amt rechtfertigen. Das Gesetz über das Bundesverfassungsgericht bedarf insoweit einer Ergänzung.

Zu Artikel 4

Berlin-Klausel

Das Gesetz enthält die übliche Berlin-Klausel.

Zu Artikel 5

Inkrafttreten und Außerkrafttreten

Diese Vorschrift regelt das Inkrafttreten des Gesetzes und das Außerkrafttreten des geltenden Bundesda-

tenschutzgesetzes. Diese Fragen können sachgerecht nur im weiteren Gesetzgebungsverfahren geklärt werden. Insbesondere erscheint es zweckmäßig, für das Inkrafttreten der Vorschriften über den Bundesbeauftragten für den Datenschutz (§§ 22 bis 28 BISG) angemessene Übergangsvorschriften vorzusehen.

Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 13 63, Herderstraße 56, 5300 Bonn 2, Telefon (02 28) 36 35 51
ISSN 0722-8333